International Journal of Computer Science and Engineering Research and Development (IJCSERD)
ISSN Print : 2248-9363
ISSN Online : 2248-9371
Volume 9, Number 3 , September – December (2018) PP: 24-33

www.prjpublication.com/ijcserd.asp

IJCSERD

© PRJ PUBLICATION

MANET (MOBILE AD HOC NETWORK) – CHALLENGES, SECURITY AND PROTOCOLS

Vikram m. Agrawal
IT Department BVM Engineering College Vallabh Vidyanagar, Anand, India

Digvijaysinh Parmar
College of Agril, Infomration Technology AAU Anand, India

ABSTRACT

Mobile ad hoc networks (MANETs) are made of composite distributed systems which comprise wireless nodes. These nodes can generously and dynamically self in mobile network topologies. So they required disaster recovery environments. Ad hoc or Mobile network is not new topic but works around in a variety of forms from last two decades. Conventionally, tactical networks have been the only communication networking application that followed the ad hoc example. This evolution generates interest for research to do more in Manet's network. This paper attempts to provide a comprehensive general idea of this dynamic field and security for them. It first explains the brief preamble of that mobile ad hoc networks and its evolutions with its architecture. The paper concludes by presenting a set of challenges and troubles requiring for MANETs network and their securities for further research in the future.

Keywords: MAC; Routing; Energy saving; Security; Performance evaluation, Mobile Node,

1. INTRODUCTION

The conception of mobile computing and communication devices (e.g., wearable computers, laptops, handheld digital devices, personal digital assistants, or cellphones) is moving an innovative change in our information society. We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ever-present Computing age in which a user utilizes, at the same time, a number of electronic platforms through which he can access all the required information whenever and wherever needed [7]. The ubiquitous devices makes wireless networks the easiest solution for their inter connection, so the wireless arena has been experiencing exponential growth in the last few years. Mobile users can use their

cellular phone to check e-mail, browse internet, GPRS, GPS; travelers with moveable devices can surf the internet from airports, railway stations, coffee shop and other public locations; researchers can switch over files and other information by connecting portable

computers via wireless LANs; at home, users can coordinate data and transfer files between portable devices and desktops.

From last some years not only mobile devices are getting smaller, cheaper, more convenient, and more configured, they also run more applications and network services which increasing the growth of mobile computing equipment market. The blowing up number of Internet and laptop users pouring this growth further [8]. Projections show that in the next couple of years the number of mobile connections and the number of shipments of mobile and Internet terminals will grow yet by another 20–50% [8].

The paper aims to advance the perceptive of MANET networks and its use. Our main research contribution provides an automated assessment process to analyze security properties. These contributions harmonize the current non-exhaustive and non-automated MANET security analysis approaches to provide a more wide-ranging security analysis potential to evaluate security properties in MANET Network. More recently, new alternative ways to deliver the services have been rising. These are paying attention around having the mobile devices connect to each other in the transmission range through automatic configuration, setting up an ad hoc mobile network that is both flexible and influential. In this way, not only can mobile nodes communicate with each other, but can also receive internet services through Internet Gateway node, effectively and securely enhancing internet services to the non-infrastructure area. Primary characteristics, such as dynamically altering topology, non-infrastructure support, resource-constrained capacity and wireless transmission, make MANETs quite different from conventional wired or wireless networks. Most accessible security methods those are valid in traditional networks but not suitable for a MANET environment. In this, we study the security at data link layer, securing routing and onforce collaboration.

This paper presents the impulsion behind mobile ad hoc networks, and presents a delegate collection of technology solutions used at the different layers of the network.

The paper is prepared as follows. In Introduction of Mobile Ad Hoc Network, we look at mobile ad hoc networks in closer detail with development, covering their specific characteristics, advantages, as well as design challenges. This is followed by a security of MANET which covers the Cross-layer research areas, including, energy management, security and cooperation, Quality of Service, and performance evaluation. Finally, we conclude the whole paper.

2. MOBILE AD HOC NETWORKS

Mobile and ubiquitous computing has been probable now due to the advances in modern wireless communication technology, aiming to provide “anywhere, anytime” communication services for users. Wireless ad hoc networking is such an sophisticated wireless transmission technology, which can be rapidly deployed in any area to provide mobile communication services without any fixed spinal column infrastructure support. By allowing multi-hop transmission, out of range communication can be achieved in wireless ad hoc networks, which reduces the requirement of the infrastructure-based backbone. In other words, a wireless ad hoc network can be easily created at anywhere when needed, particularly in places where infrastructure-based communication system cannot be shaped due to geographical or terrestrial constraints.

2.1. Manet Advancement

In history, mobile ad hoc networks have principally been used for creating new art of network organization where either the infrastructure is gone or where position an infrastructure is not

very cost effective [2]. Pure wireless communication also has restriction in that radio signals are subject to intrusion and radio frequency higher than 100 MHz not often promulgate beyond line of sight (LOS) [9]. Mobile ad hoc network creates a appropriate structure to address these issues by providing a multi-hop wireless network without pre-placed infrastructure and connectivity ahead of LOS. The whole life-cycle of ad-hoc networks could be divided into the First, Second, and the Third generation ad-hoc networks systems. Present ad-hoc networks systems are considered the Third generation.

The first generation goes back to 1972. At the time, they were addressed PRNET (Packet Radio Networks) developed by DARPA. The PRNET used a mixture of ALOHA and CSMA approaches for medium access, and a type of distance-vector routing.

The second generation of ad-hoc networks emerged in 1980s, when the ad-hoc network systems were additional improved and implemented as a part of the SURAN (Survivable Adaptive Radio Networks) program which was developed by DARPA. This provided a packet-switched network to the mobile battleground in an environment without infrastructure. SURAN was developed to conquer the problem of PRNET like network scalability, security, processing capabilities and energy management. The main objectives were to develop network algorithms to support a network that can scale to tens of thousands of nodes and endure security attacks, as well as use small, low-cost, low-power radios that could support sophisticated packet radio protocols [9]. This effort consequences in the design of Low-cost Packet Radio (LPR) technology in 1987 [10],

In the 1990s, the idea of commercial ad-hoc networks arrived with notebook computers and other practical communications equipment. At the same time, the idea of a set of mobile nodes was projected at several research conferences.

The IEEE 802.11 subcommittee had adopted the term "ad-hoc networks" and the research community had in progress to work on the likelihood of deploying ad-hoc networks in different areas of function. In the early 1990s a epidemic of new developments signaled a new stage in ad hoc networking. Notebook computers became well-liked for feasible communications equipment based on RF (Redio Frequency) and infrared. The idea of an infrstructureless collection of mobile hosts was planned in two conference papers [11, 12] and the IEEE 802.11 subcommittee adopted the term “ad hoc networks.” The idea of commercial (non-military) ad hoc networking had inwards.

At around the same time, the DOD in progress where it left off, financial support programs such as the Global Mobile Information Systems (GloMo), and the Near-term Digital Radio (NTDR) The aim of GloMo were to give connectionless Ethernet kind environment in office as anytime, anywhere, in portable devices such as mobile, tablet, computer and GPS. Channel access approaches were now in the CSMA/CA and TDMA molds, and a number of narrative routing and topology control schemes were developed. The NTDR used clustering and link- state routing, and self-organized into a two-tier ad hoc network [3]. The US Army is used NTDR today only, it is the merely “real” non-prototypical ad hoc network. The rising interest in ad hoc networking has optimistic a number of standards and commercials behavior to evolve in the mid to late ’90s. The Mobile Ad Hoc Networking (MANET), in IETF, operational group developed, and sought to regulate routing protocols

for ad hoc networks. The growth of routing within the MANET working group and the bigger community branched into reactive (routes on- demand) and proactive (routes ready-to-use) routing protocols [4]. The 802.11 subcommittee standardized a medium access protocol that was based on collision avoidance and tolerated hidden terminals, making it usable, if not most favorable, for building mobile ad hoc network prototypes out of notebooks and 802.11

PCMCIA cards. HIPERLAN and Bluetooth were some other standards that addressed and benefited ad hoc networking [3].

2.2 Ad hoc networking issues

There are some specific MANET issues and constraints which create evils and significant challenges in ad hoc network plan. To present the enormous amount of research activities on ad hoc networks in a methodical way, we will use, as a suggestion, the simplified architecture shown in following Fig. [1].

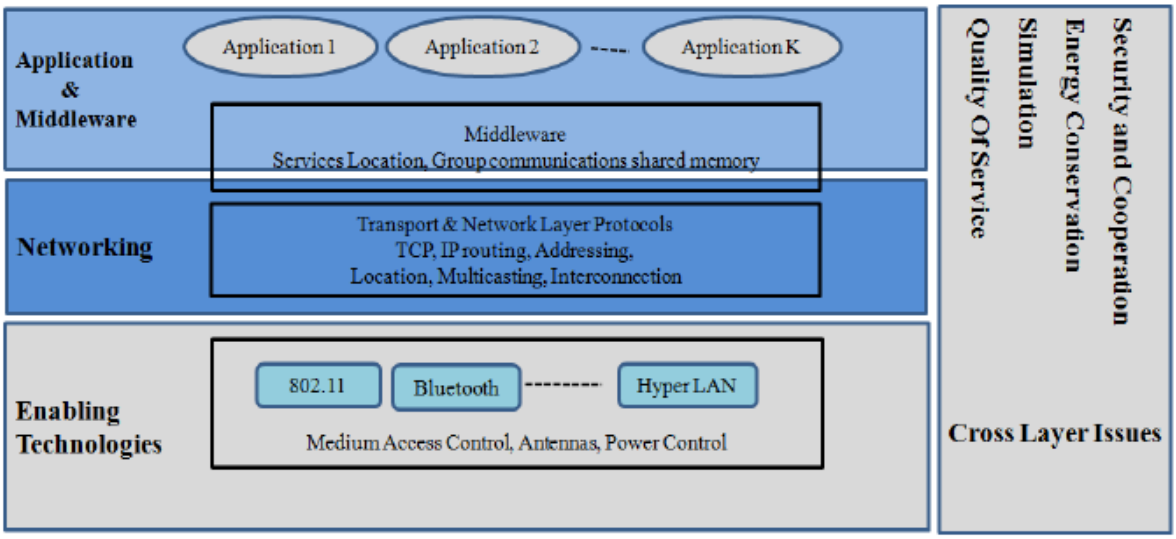

Figure 1 Simple architecture for Ad Hoc Network

As shown in the figure, the research activities will be conbined, according to a layered approach into three main areas:

• Enabling technologies; • Networking; • Middleware and applications.

In addition, as shown in the figure, a number of issues (energy management, security and cooperation, quality of service, network simulation) extent all areas, and we discuss them independently [1].

3. NETWORK SECURITY AND COOPERATION

In MANETs, all the nodes are infrastructureless so by nature they are wireless mobile ad hoc, so we neeed to look new security challenge to the network plan. We also need to sacrifies the information and security in wireless ad hoc network than permanent wired networks. Susceptibility of channels and nodes, lack of infrastructure and vigorously altering topology, make ad hoc networks security a difficult job [13]. Nodes do not exist in in physically protected places, and so they can be easily attacked by the attacker and forbidden by them. The absence of infrastructure makes the traditional security solutions such as certification

establishment (Maintain by the some central Authority) and on-line servers unsuitable (which maintian the nodes information). Lastly, the security of routing protocols in the MANET dynamic environment is an supplementary challenge.

The self-organizing environment introduces new security issues that are not included in basic security services provided in wired networks. So the security accessible in MANET is not good adequate for rightness and integrity of information which are shared. A basic necessity for keeping the network prepared is to enforce ad hoc Nodes involvement to

network operations, in spite of the conflicting propensity (motivated by the energy motivated) of each node towards selfishness [14,15].

3.1. Security attacks

Securing wireless ad hoc networks is a large challenge. Before preparatory to provide security in MANET or any ad hoc network, it is essential to understand probable form of attacks. Ad hoc networks have to cope with the similar kinds of vulnerabilities as their wired counterparts, as well as with new vulnerabilities specific to the ad hoc context [16]. In addition, traditional vulnerabilities are also noticed by the ad hoc prototype.

The difficulty and variety of the field (different applications have different security constraints) led to a huge number of proposals that can not be all surveyed in this editorial. Comprehensive analyses of ad hoc networking security issues and solutions can be found in [13, 17, and 18]. Underneath we summarize how to classify the attacks. The following Figure shows a classification of possible security attacks in MANETs.

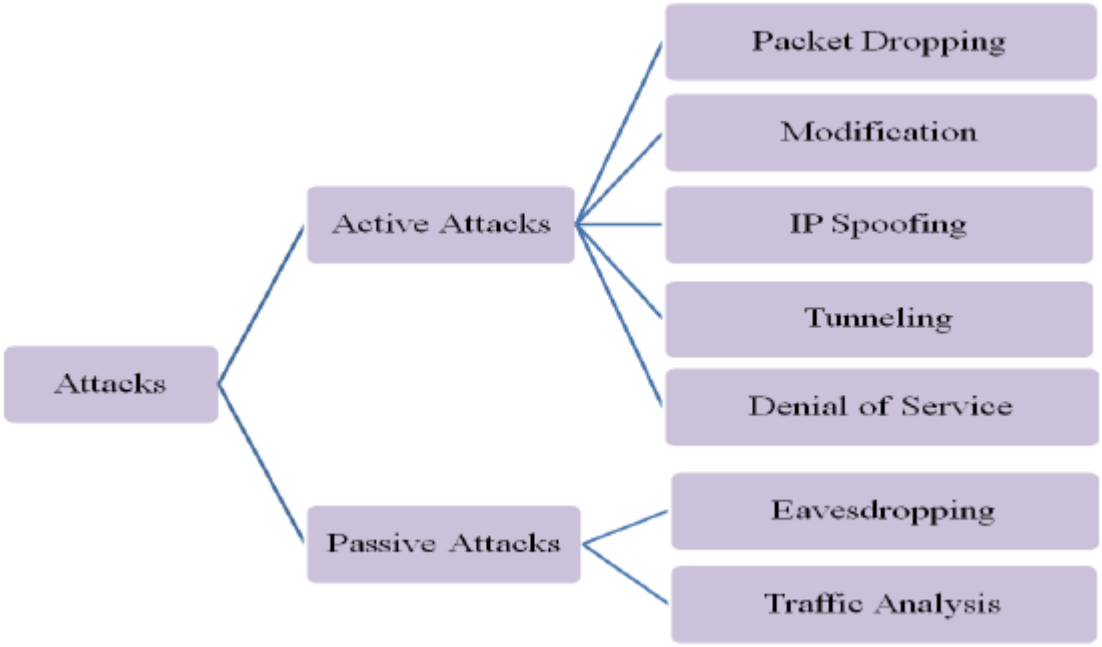

Figure 2 categorization of Attacks

Performing communication in free space exposes ad hoc networks to attacks as anyone can join the network, and eavesdrop or insert messages. Ad hoc networks attacks can be classified as inactive or active [19].

Active attack can be defined as “the attacker or impostor modify or alter the data which can be shared among the nodes in the networks”. In a MANET, an attacker humiliate the network performance by inappropriately modifying the routing message, injecting mistaken messages, or pretending an authorized Mobile Node to confuse the normal network

procedure. Active attacks can be further categorized as routing disruption attacks and resource consumption attacks depending on the purpose of the attackers. In routing disturbance attacks, the attacker send legal bits or packets in a malicious way; while in resource utilization attacks, the attacker aims to gain precious network resources, such as radio bandwidth, users’ energy, memory space and computational power. Depending on the events taken by an attacker, active attacks can be classified into several common attack subcategories as follows.

Packet dropping: An intruder pretends to be Mobile Node or genuine user itself from others Mobile Nodes. In this attacker will throw away or destroy all the packets which are routed to him. This is identified as black hole attack. In black hole attack, attacker sends fake routing packets, so that it can route all the packets for some destinations to itself, and then remove them. As a special case, an attacker can decide selective packets and drop them as a substitute of discarding all packets, thus creates a grayhole attack.

Modification: A spiteful node modifies message throughout the transmission between the communicating nodes, For example, an attacker can deliberately shorten or lengthen the node list in the routing packet, curtail or lengthen the messages.

IP spoofing: A spiteful node sends a internet protocol packet containing its own MAC address and a victim's IP address, thereby usurping the IP-to-MAC address

binding of the victim from the other neighbor's Address Resolution Protocol (ARP) cache.

Tunneling attack: A spiteful node creates a different type of routing disturbance, called as tunneling attack [20], and by using a pair of spiteful nodes connected together via a private network connection. Every packet node a received can be forwarded to node b through their private connection. This attack can potentially disturb routing by shortcircuiting the usual flow of routing packets. It means that if authorized sender sends packets, it will be catched by private network of intruder being receiver and then intruder send smashed packets to authorized receiver.

DoS: An attacker can mount a replay attack by sending old messages to a destination node again and again, aiming to excess the network and wear out the node's resources. Moreover, an attack can generate a speeding up attack in this he sends routing request packets with high frequency to find real route and keep other nodes busy. The reason here is to make the network service not available for other lawful or authorized nodes. The Routing Table Overflow and the Sleep Depravation attacks [236, main peper] fall in this class.

Passive attack: is an attack where an unofficial attacker monitors or listens to the communication among two parties. It means that attacker or intruder never send any corrupted message in a MANET network. An attacker may inactively listen to the network traffic to collect valuable information, such as network connectivity, node location, traffic distribution, and so on. The main goal of passive attacks is to generate threat against the network privacy. Compared with active attacks, passive attacks are very tough to prevent and detect because the intruders are not concerned in any change of transmitted message or disruption of the network activity. Depending on

dissimilar actions taken by an attacker, passive attacks can be further separated into following subcategories.

Eavesdropping: An attacker can get direct knowledge of the network by intercepting transmitted data packets. Passive eavesdropping can be prohibited by a variety of encryption schemes and defensive the privacy of the data transmission, so attacker can not recognize the encrypted data and its' key.

Traffic analysis attacks: An attack may dig out valuable information from the distinctiveness of the transmission such as node identity, the amount of transmitted packets, time required to send one bit or a packet and the frequency of data transmission. The extracted information may allow the attacker to do a auxiliary analysis and figure out some sensitive knowledge [21, 22].

3.2. Basic security mechanisms:

Essentially there are two types of security in wired and wrireless: preventive and detective. The defensive mechanisms mean we can try to stop unconstitutional access in our shared network. Defensive mechanisms are classically based on key-based cryptography. Keys delivery is main point for these mechanisms. Secret keys are dispersed through two methods one is symmentric and other is asymmetric. We need to set up secure channel for sharing key in symmetric cryptography but it is difficult to apply in ad hoc networks. In asymmentric, we use public key distribution. An asymmetric cryptography means, there two keys one is public key and other is private key. A public key can be shared among all the parties who are in network and private key is only secure with particular user. Public keys are dispersed through certificates that bind a public key for network users. In the centralized approach, certificates are provided, stored, and distributed by the Certificate Authority (CA). Because no central authority no centralized trusted and third party and server are probable in MANET, the key management purpose needs to be distributed over Nodes. The server takes the accountability for key management shared among a set of Nodes [24]. The challenge of creating such a confidence mixture does not depend on only costructing and configuring the aggregation, but it is also depends on hoe we provide security to such aggregation when the network topology is changed with moving or mobile users, Although we can create a completely distributed self organizing public key management system for MANETs [23]. In this approach the users issue certificates for every other based on their personal links. Certificates are stored in a local certificate database and dispersed by the users themselves. When two users want to verify the public keys of each other, they combine their local certificate databases. The authors analyze the vulnerabilities of key-based security mechanisms, and suggest solutions to defend these mechanisms [16].

The discovery mechanism means we just find out that where the illegal activities are happened. Most of the imposition detection techniques developed on a fixed wired network are not applicable on MANETs. In ad hoc network there are no traffic consciousness points like switches, routers, etc. where the intrusion detection system (IDS) can gather inspected data for the whole network. In mobile ad hoc network IDS require to depend on only accessible audit information which was composed within the radio variety So the intrusion detection algorithm must rely on this incomplete and localized information. A proposal for a new intrusion detection structural design that is both distributed and cooperative is presented in [25, 26]. To find out the intrusion detection in MANET, all the authorized users contribute in intrusion detection and response. Each node is in charge for detecting symbols of attacks

locally and separately, but when neighbors want to detect intrusion, they need to create collaboratively study in a broader range.

3.3. Security at data link layer

Bluetooth and 802.11 apply mechanisms based on cryptography to stop unauthorized accesses, and to advance the privacy on radio links. An investigation of the various 802.11 and Bluetooth mechanisms can be found in [18].

Security in the IEEE 802.11 standard is provided by the Wired Equivalent Privacy (WEP) scheme which provide the security same as wired security. WEP provides both data encryption and integrity. So when data is sent and received by two parties, are in real form. The security is based on a 40-bit secret key. The secret key can also be a default key shared by all the devices of a WLAN in asymmetric encryption, or a pairwise secret key shared only by two communicating devices in symmetric encryption. Since WEP does not provide any support for the exchange of secret keys, the secret key must be manually shared by authorized

communicating parties. As WEP suffers from various design flaws and weaknesses [18], So IEEE 802.11 standardization is designing the new 802.11 security architecture for correcting problems.

Bluetooth uses cryptographic security mechanisms implemented in the data link layer. A key management service provides each device with a set of symmetric cryptographic keys necessary for the initialization of a secret channel with another device, the implementation of an authentication protocol, and the switch over of encrypted data on the secret channel. A thorough presentation of Bluetooth security mechanisms, together with an analysis of the weaknesses in the Bluetooth key management scheme can be found. [18]

3.4. Secure routing

The spiteful nodes change the information about the routing protocol for disrupting the accurate performance information. They also try to imagine other nodes to share the packets. Modern studies [27] brought up also a new type of attack that goes under the name of wormhole attack mentioned earlier.

We next sum up the recent research that has been done in order to come up with secure routing protocols for ad hoc networks. [28, 18] The Secure Routing Protocol [29] is conceived as an addition of simple routing protocol. It menas the security application can be applied to numerous existing routing protocols. SRP is based on the supposition of the being of a security association between the sender and the receiver based on a shared secret key negotiated at the connection setup. SRP fights with attacks that disrupt the route discovery process. A node initiating a route discovery is capable to identify and discard false routing information. Likewise to SRP, Ariadne [30] assumes that each pair of communicating nodes has two secret keys (one for each direction of the communication). So that when we use Ariadne protocol, that time both users uses secret key to send information to receivers. Ariadne is a secure ad hoc routing protocol based on DSR (Dynamic Source Routing) and the TESLA (Timed Efficient Stream Loss-tolerant Authentication protocol) [31].

The Authenticated Routing for Ad hoc Network (ARAN) protocol is storng protocol to provide defensive and detective security for MANETs. It is secure, routing protocol that detects and protects alongside malicious actions carried out by third parties in the ad hoc surroundings [32]. ARAN is based on certificates mechanism which is provided by the

trusted certificate server and later on allowed to join ad hoc network. ARAN utilizes a route discovery process similar to AODV (Ad Hoc on demand Distance Vector Routing). The route discovery develops en to end authentication among two authorirized nodes and assure that merely destination node can respond to a route discovery packet.

The Secure Efficient Ad hoc Distance (SEAD) is a practical secure routing protocol based on DSDV (Deastination Sequensed Distance Vector). SEAD deals with attackers that modify a routing table update message. The basic idea is to authenticate the sequence number and the metric field of a routing table keep informed message using oneway hash functions [33]. Hash chains and digital signatures are used by the SAODV mechanism to secure AODV [34].

4. CONCLUSION

The development of MANET cannot be divided from the the world of computing. Since it is portable and compact media with which we can communicate exclusive of wired network. In this review paper we discussed some typical and dangerous vulnerability in the MANET, attack types security criteria, which move on to supply guidance to the security-related research works in this area. Due to the absence of a clear line of protection or communication in MANETs, a complete security solution for them should integrate both proactive and

reactive approaches. The solution should cover of all three mechanisms: prevention, detection and reaction. It means when we want to provide secure communication channel in MANET that time it must secure sufficient to prevent unauthorized penetration, sense where the intrusion is occurred and give proper action to that intrusion or attack. The MANETs security issues endorse new ideas. It has got impending widespread applications in military, corporate and civilian communications. In these networks all the nodes are helpfully dependant to perform networking function. This paper mentions many secure protocol which can be used to provide cryptogrsphy and time based security. One such misconduct is related to routing of packets. When such unruly nodes take part in the route discovery process, but refuse to forward the data packets, routing performance may be tainted cruelly.

REFERENCES

[1] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Ad Hoc Networks 1 (2003) 13–64, “Mobile ad hoc networking: imperatives and challenges”, 2003.

[2] Humayun Bakht, “The History of mobile ad-hoc networks, Wireless Infrastructure”, 1, Augast, 2005<http://zatz.com/computingunplugged/article/the-history-of-mobile-ad-hoc-networks/>

[3] A brief overview of Ad Hoc Networks: Challenges and Directions, Ram Ramanathan and Jason Bedi, BBN Technologies, IEEE Communication Magazine 50th Anniversary Commemorative Issue/May 2002

[4] E. Royer and C.-K. Toh, "A Review of Current Routing 'Protocols for Ad Hoc Mobile Wireless Networks,"IEEE Pers. Common., vol. 6, no. 4, Apr. 1999, pp 46-55.

[5] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.

[6] A. Ahuja et al., Performance of TCP over different routing protocols in mobile ad-hoc networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC 2000), Tokyo, Japan, May 2000.

[7] M. Weiser, the Computer for the Twenty-First Century, Scientific American, 1991.

[8] Wireless World Research Forum (WWRF): http:// www.ist-wsi.org.

[9] James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed .), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

[10] W. Fifer, F. Bruno, The low-cost packet radio, Proceedings of the IEEE 75 (1) (1987) 33–42

[11] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM '94, Oct. 1994.

[12] D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," Proc. ACM

[13] L. Buttyan, J.P. Hubaux, Report on a working session on security in wireless ad hoc networks, Mobile Computing and Communications Review 6 (4) (2002).

[14] S. Giordano, A. Urpi, Self-organized and cooperative ad hoc networking, in: S. Basagni, M.Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003

[15] P. Michiardi, R. Molva, Simulation-based analysis of security exposures in mobile ad hoc networks, in: Proceedings of European Wireless Conference, 2002.

[16] J.P. Hubaux, L. Buttyan, S. Capkun, The quest for security in mobile ad hoc

[17] networks, in: Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October 2001.

[18] M. Ilyas, Handbook of Ad Hoc Networks, CRC Press, New York, 2003.

[19] P. Michiardi, R. Molva, Ad hoc networks security, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[20] J.Lundberg, Routing Security in Ad Hoc Networks, 2000. Availabe from http://citeseer.nj.nec.com/ 400961.html

[21] A. Perrig, Y. C. Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks,"Technical Report TR01-384, Department of Computer Science, Rice University, December 2001.

[22] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," H. Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 10-29, Springer-Verlag, 2000.

[23] S. Jiang, N. Vaidya, and Wei Zhao, "Prevent Traffic Analysis in Packet Radio Networks," in Proceedings of DISCEX II, June 2001.

[24] S. Capkun, L. Buttyan, J.P. Hubaux, Self-organized public-key management for mobile ad hoc networks, IEEE Transactions on Mobile Computing 2 (1) (2003).

[25] L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network Magazine 13 (6) (1999).

[26] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the Sixth ACM International Conference on Mobile Computing and Networking (MOBICOM 2000), Boston, MA, USA, August 6–11, 2000.

[27] Y. Zhang, W. Lee, Y. Huang, Intrusion detection techniques for mobile wireless networks, ACM/Kluwer Mobile Networks and Applications (MONET) 9 (5) (2003).

[28] A. Perrig, Y.-C. Hu, D.B. Johnson, Wormhole protection in wireless ad hoc networks, Technical Report TR01-384, Department of Computer Science, Rice University.

[29] Elizabeth Belding-Royer, Routing approaches in mobile ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.

[30] P. Papadimitratos, Z. Haas, Secure routing for mobile ad hoc networks, in: Proceedings of CNDS, 2002.

[31] Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: a secure ondemand routing protocol for

[32] ad hoc networks, in: Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (MOBICOM 2002), Atlanta, GA, September 23– 28, 2002.

[33] A. Perrig, R. Canetti, J.D. Tygar, D. Song, Efficient authentication and signing of multicast streams over lossy channels, in: Proceedings of IEEE Symposium on Security and Privacy, 2000.

[34] K. Sanzgiri, B. Dahill, B.N. Levine, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[35] Yih-Chun Hu, David B. Johnson, Adrian Perrig, and SEAD: secure efficient distance

[36] vector routing for mobile wireless ad hoc networks, in: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCS a 02), New York, and June 2002.

[37] European Commission, FET-IST Programme, MobileMAN project (IST-2001-38113). Available from <http:// cnd.iit.cnr.it/mobileMAN/ >

[38] Dmitri D. Perkins, Herman D. Hughes, A survey on quality of service support in wireless ad hoc networks, Journal of Wireless Communication & M obile Computing (WCMC), Special Issue on Mobile Ad Hoc Networking: Research, Trends, and Application 2 (5) (2002) 503–513.

[39] R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, K. Thurber, Techniques for intrusion-resistant ad hoc routing algorithms (TIARA), in: Proceedings of MILCOM, October 2000.