On Recent Security Enhancements to Autoconfiguration Protocols for MANETs Real Threats and Requirements

A. Abdelmalek [1], M. Feham [1] and A. Taleb-Ahmed [2]

[(1)] STIC Laboratory, University of Tlemcen, Algeria
[(2)] LAMIH Laboratory, University of Valenciennes and Hainaut Cambrésis, France

Summary
In the context of Mobile Ad hoc Networks (MANETs) security, most of research so far has been focused primarily on trust models and routing security problems, and much less attention has been given to the autoconfiguration security issue. However, the lack of security in the design of all previously proposed autoconfiguration schemes opens the possibility of many real threats, due to the well-known MANETs' vulnerabilities which are specific to ad hoc paradigm. This can lead hence to serious attacks in potentially hostile environments, such as IP Spoofing Attack, Exhaustion Address Space Attack, Conflict Address Attack, Sybil Attack, etc. Few papers have tackled this problem without however bringing satisfactory solutions. In this paper, we first present a survey of these approaches, and discuss their limitations. Then, we define the imperative security requirements in designing and implementing any solutions addressing this still open issue.

Key words:
Autoconfiguration, Threats, Security Requirements, Mobile Ad Hoc Networks.

1. Introduction and Background

Mobile ad hoc networks (MANETs) are an ideal technology to deploy spontaneous wireless infrastructure-less networks, either for military or civilian applications. Deployment of such networks requires the implementation of mechanisms for initial configuration of the participants with some network and security parameters. In particular, when new node joints a MANET, it must be assigned a free IP address before it may take an active part in the network. This fundamental and difficult problem has received large consideration in the few last years, and several autoconfiguration solutions have been developed to deal with the following problems: address uniqueness, network initialization, address leakage, node departures, network partitioning and merging, and to address also efficiency and scalability (refer to [1], [2] for a survey). In general, we can categorize these solutions to be either stateful or stateless. In stateful schemes, the IP address is assigned by the network (i.e. by either one node or a set of nodes belonging to the network), thus the network has to maintain state information about already used and/or free addresses. Binary Split/Buddy System approach proposed by A. Misra et al. [6] and improved by M Mohsin et al.[5] is one of the most interesting stateful solutions. In this scheme nodes hold disjoint address pools using the concept of binary split. Consequently, each node can independently configure any newly arrived node with an unassigned IP address and a pool of free addresses without consulting any other node in the network.
Another approach (MANETconf) based on the principle of Distributed DHCP was proposed by S. Nesargi and R. Prakash [10]. In this scheme, the functionality of DHCP is distributed over the entire network; nodes have the same address pool, which means they must maintain global allocation state information. When a new node (requester) joins the network, one of its neighbors (initiator) could choose a free address for it. As a same free IP address in the address pool could be assigned to two or more new nodes at the same time by different configured nodes, a duplicate address check is necessary.

A stateful function based scheme called Prophet Address Allocation was developed by H. Zhou et al. [7]. The stateful function generates IP addresses such that the probability of conflict address is very low. The first node (prophet) chooses randomly an IP address and an initial seed. These values are used as input for the stateful function to derive new IP address and new seed for any newly joining node.

On the contrary in stateless schemes, the IP address is assigned by the node itself which has to perform a uniqueness test to find out whether there is a duplication conflict. Among the most relevant work in stateless solutions, we note first Strong DAD approach proposed by C. Perkins et al. [16]. This solution based on a random choose of tentative IP address from a predefined address pool, and followed by an address uniqueness check carried out with a Duplicate Address Detection (DAD) protocol, requesting approval from all the nodes of the network. Next, we have Strong-Weak DAD approach proposed by J. Jeong et al. [17]. This solution proposes two Duplicate Address Detection processes. The first one (Strong DAD) is performed in the initial autoconfiguration phase to check address uniqueness, whereas the second

Manuscript received April 5, 2009
Manuscript revised April 20, 2009

one (Weak DAD) is proactively done during the routing process to handle merging networks. Another stateless approach developed by K. Weniger, called PACMAN [26] proposes an address assignment using a probabilistic algorithm, and passive duplicate address detection based on anomalies in routing protocol traffic. Finally, the class of Leader based approaches (K. Weniger and M. Zitterbart [4] and Y. Sun and E. M. Belding-Royer [9]) is also interesting. Instead of all nodes have to participate in DAD process, in these scheme the responsibility is given to special elected nodes (leaders [4] or Address authority [9]). Allocation state information must be maintained by leaders which periodically broadcast necessary information to allow a new joining node to be configured, to ensure address uniqueness and to handle network partitions and merges.

Depending on size topology and network dynamics, each one of the above solutions has its advantages and drawbacks (refer to [1], [3] for details). However, they all suffer from a common problem: lack of security. Much less attention has been given to security in the design of such schemes. Thus, vulnerabilities related to the particular features of MANETs [11] may be exploited by an adversary to perform passive and active attacks, influencing the whole network availability and behavior.
Recent studies [11]-[15] have presented few tentative schemes to solve this problem, but none of them has brought satisfactory solutions. The autoconfiguration security issue is still an open problem. The purpose of this paper is to identify all possible threats and to define throughout the analysis of previous related work the imperative security requirements in designing such schemes.

The paper is organized as follows. Section 2 presents possible attacks on proposed autoconfiguration schemes. In section 3, we review and analyze existing solutions for securing autoconfiguration protocols, while presenting their limitations and shortcomings. In section 4, we identify desirable design proprieties to be fulfilled by any secure autoconfiguration scheme for MANETs. Finally, section 5 concludes the paper.

2. Security Threats

In all proposed autoconfiguration schemes for MANET, the service functionality depends on the correct behavior of the participating nodes. However, in reality, malicious nodes may be present in the network, potentially causing a variety of possible problems. Following [6] and [13], we identify several attacks (Table-1 shows concerned above approaches with these attacks):

2.1 IP Spoofing Attack

A malicious node could either spoof an already assigned or a free IP address. In the former case, it spoofs any configured node and hijacks his traffic; in the latter case, it assigns itself a free valid IP address to participate in the network, to get some information by performing active attack or to cause at least Denial-of-Service (DoS) attacks.

2.2 Exhaustion Address Space Attack

A malicious could claim as many IP addresses as possible to exhaust Address Space. It could also request address allocation for phantom nodes (i.e. nodes that do not exist). By acquiring all valid addresses, it can deny others nodes to be configured.

2.3 Conflict Address Attack

A malicious node could assign to a requester a duplicate address with possibly a pool of already used addresses. It could perform, in the DAD process, a black hole attack for Address Replay (AREP) messages. This can lead to serious Conflict Addresses in the network.

2.4 False Conflict Address Attack

A malicious node could replay, in the DAD process, to Address Request (AREQ) message with false conflict Address Replay (AREP) message claiming that the candidate IP address is already assigned; it may if necessary change temporarily its IP address to perform this attack.

2.5 Sybil Attack

Sybil attack is a particularly harmful attack in MANETs where a node illegitimately claims multiple identities. A Sybil node can either fabricate a new identity or steal an identity from a legitimate node. Getting several IP addresses by a Sybil node facilitate much its attack. This is, indeed, possible with the above mentioned autoconfiguration mechanisms. According to the protocol used, a Sybil node could either claim or assign itself many IP addresses.

2.6 Traffic overload DoS Attack

In a requester-initiator scheme, a malicious node could act as a requestor and send Address Request messages to

many initiators simultaneously. A malicious node could also send many DAD messages for many candidate IP addresses, resulting in traffic overload.

Table 1: Possible attacks on existing autoconfiguration schemes

	IP Spoofing Attack	Exhaustion Address Space Attack	Conflict Address Attack	False Conflict Address Attack	Sybil Attack	Traffic overload DoS Attack
Binary Split	YES	YES	YES	NO	YES	NO
DDHCP	YES	YES	YES	YES	YES	YES
Prophet	YES	YES	YES	NO	YES	NO
Strong DAD	YES	YES	YES	YES	YES	YES
Strong-Weak DAD	YES	YES	YES	YES	YES	YES
PACMAN	YES	YES	YES	NO	YES	NO
Leader Based	YES	YES	YES	YES	YES	NO

3. Survey and Analysis of Previous Securing Schemes

To the best of our knowledge, [11]-[15] are the only existing papers dealing with IP address autoconfiguration security issue. A short review of these papers is presented in this section, followed by an analysis highlighting the limits of the proposed solutions.

3.1 One hop On-line Certification Authority [11]

First, F. Buiati et al. have presented in [11] a security extension to Dynamic Configuration and Distribution Protocol DCDP also known by the concept of binary split or buddy system [5],[6]. Their proposal is based on the imposition to new joining nodes to get an On-line certificate before applying for, or participating in autoconfiguration service. This certificate binds the identity of a node to his public key, and is obtained from a distributed Certification Authority in a one-hop (k,n) threshold trust model (i.e. the certificate is signed by at least k trusted neighbor nodes out of n nodes in the whole network). In the autoconfiguration process, all autoconfiguration protocol messages must be authenticated with non repudiation. This is achieved by a MANET Authentication Extension MAE [19] appended to each message.

The mean problem of the proposed solution is that the certificate service availability is not guaranteed. For a new joining node, finding at least k trusted neighbor nodes is not always possible. That is one of the drawbacks of this solution.

To ensure the correct operation of the autoconfiguration service, the authors proposed two other security requirements: detection of misbehaving actions against autoconfiguration service, and generation of accusation against adversary nodes. But they did not give any mechanism for this purpose. According to [6] every node in the network must keep a table with node identifier and assigned IP addresses, to keep track of the assigned IP addresses. It is not shown how to securely construct these tables. As a result, the solution proposed does not allow preventing Exhaustion Address Space and DoS Attacks.

The authors did not treat also in their solution the IP Spoofing Attack. A malicious node with a valid certificate can easily spoof already used IP addresses to hijack traffic or to perform some attacks like conflict Address Attack or Sybil Attack. (Note that the IP spoofing Attack can be prevented if the above IP tables are securely maintained).

3.2 Pré-Authentication and threshold Authorizations [12]

A. Cavalli and J-M Orset have proposed in [12] another autoconfiguration security solution applied to buddy system model [6]. A new joining node requesting an IP address and a pool of free addresses must first of all collect a threshold of authorizations from its one-hop neighbor nodes. Each authorization is given following a mutual authentication between the requester node and each neighbor node. We have find four problems with this solution:

−A newly arrived node is not always able to have a sufficient number of one-hop neighbor nodes (i.e. a number greater than threshold number).

−The IP address and the pool of free addresses are finally attributed by only one neighbor node which claims to hold the big pool of addresses. This node may be a malicious node.

−The requester may also be malicious, the solution proposed by the authors is not protected against the Exhaustion of Address Space Attack (consider a mobile adversary model [11]).

−The authors have not addressed any mechanism to thwart IP Spoofing Attack. Indeed, a malicious node could at any time spoof any valid IP address to take an active part in the network or to just hijack traffic, since there is no mechanism to check whether the IP address is bound to node's identity.

3.3 Hashed public key based IP address [13]

P. Wang et al. [13] have described an original self-authentication scheme for address autoconfiguration, which binds a node's IP address with a public key via a one-way hash function. A node's IP address is obtained by

hashing its public key. The scheme uses also the Duplicate Address Detection (DAD) process to check IP address uniqueness. To solve the problem of collisions, the authors proposed to retry with new pairs of public/private keys. The proposed solution presents also some drawbacks:

–The proposed scheme is stateless, and so any node can generate an IP address all alone to take part in the network.

–Taking into account the collision problem, the public keys are generated as much as that is necessary, and they are not signed by any Certification Authority. This gives the possibility to malicious node to have several public keys and several IP addresses; thus it can easily perform Sybil attack.

–A malicious node may beforehand generate randomly several pairs of public keys and associated IP addresses and save them in a table. Then, it performs False Conflict Address Attacks. When receiving a Duplicate Address Detection Request, it just verifies if the IP address (target address) in the received message corresponds at any address of its table, then it performs the attack by changing its IP address to the target one.

–The authors point out the necessity of nodes authentication to counter IP Spoofing Attack, but their solution does not deal with this attack. We suggest that each new generated public key has to be signed by an On-line Certification Authority. Besides, we question ourselves how that can be carried out.

3.4 Trust value based Trust Model [14]

Recently, S. Hu and C.J. Mitchell [14] have proposed to use a trust value based Trust Model to improve the security of requester-initiator schemes for IP address autoconfiguration in MANETs [10]. In this model, each node i maintains a threshold trust value T_i^*, and it deems a node j as trustable if and only if the trust value $T_i(j)$ hold by node i for node j is such as : $T_i(j) \geq T_i^*$, otherwise it is considered as malicious.

Each node keeps also a blacklist containing identities of malicious nodes. This blacklist is dynamically updated using information gathered. To choose a trustable node (say i) as the initiator, the authors propose to combine trust values hold by neighbor nodes for node i. To check IP address uniqueness, Duplicate Address Detection (DAD) Protocol is performed. To secure this process, the initiator uses the trust value it holds/calculates for the responder node.

To deal with some of the vulnerabilities in their model, the authors make many assumptions which are not realistic in a hostile environment, what weakens their solution and makes it unsuited for MANETs. Indeed, we raised some drawbacks and lacks of security which we summarize in the following points:

– To quantify trust, each node must calculate trust values of its neighbor nodes or other multi-hops nodes. In the first case, the calculation is based on information gathered and accomplished by passive observation by the node about the behavior of neighbor nodes. This approach is not efficient seen that it is based on the analysis of traffic. The authors add also that potential problems could arise in this process regarding the density of nodes and MAC layer protocols being used. In the second case to determine trust value for a multi-hops node i.e a non-neighbor node, the authors propose to modify the DSR protocol [18] Route Discovery Method by adding a trust list containing trust values for each node in the route record. Each node in the route record must append a trust value for its successor. This approach is vulnerable to integrity attack. A malicious node can intentionally change the trust values list. Even if it will be easy to learn that there is at least one malicious node in the route, it is not possible to identify it. This will force the initiator to repeat the DAD process resulting in a DoS attack, precisely in latency.

–The authors claim that the probability that a malicious node will be chosen as initiator is low, accepting that a majority of the nodes in the network are honest nodes. This assumption is not founded. Indeed, consider the case of a set of neighbor nodes in which the majority of nodes are malicious/compromised, the probability above will depends so on the distribution of malicious/compromised nodes even if they are minority in the network.

–To cause a DoS Attack, a malicious node could act as a requester and sends Address Request messages to many initiators simultaneously. The approach described previously cannot prevent this type of attack.

–As pointed out by the authors themselves, the proposed model suffers from Sybil and IP spoofing attacks, and it is also vulnerable to malicious nodes which behave maliciously only with respect to trust model functionality.

3.5 Primary Address Authority's messages signature [15]

To our best knowledge, the most recent work dealing with security problems in autoconfiguration in MANETs has been presented by A. Langer and T. Kühnert [15] to secure the Optimized Dynamic Address Configuration Protocol ODACP [8]. The protocol ODACP uses a Duplicate Address Detection Protocol combined with a leader-based scheme. The leader-based approach has been introduced to solve temporally not connected nodes which cannot send an Address Replay message in DAD process.

It is based on the so-called Primary Address Authority PAA which is elected by nodes in the network. The solution described in [15] is mainly based on two mechanisms:

First, to prevent a malicious node to send arbitrary message to other nodes which seems to have its origin at the PAA, or to send modified PAA's messages to the requester node, an encrypted checksum is added by the PAA to any address replay message (AREP). Secondly, to prevent malicious requester behavior (Exhaustion of Address Space Attack) the authors introduced a requester counter and a timestamp (last request time) as additional data fields in the IP address table of the PAA, and claim that a good threshold for the counter value will be 6 to allow a node to retry its autoconfiguration in the event of faults or communication problems.

The proposed solution [15] presents some weaknesses:

–No trust model has been defined by the authors who assume thus no authentication for address request (AREQ) message neither in DAD protocol nor in address registration. This can lead to several attacks (IP spoofing attack, MAC spoofing attack, Exhaustion of Address Space Attack).When a node obtains an IP address using DAD process, it unicasts a registration request to PAA including its acquired IP address, its MAC address and a request lifetime for the IP address. Even if the authors have added a requester counter to the IP address table of the PAA, it is obviously insufficient to prevent a malicious node to perform an exhaustion of address space attack, since neither the address request nor the address registration is signed. In order to do so, the malicious node could simply transmit false MAC address. It could also perform a MAC spoofing attack by retransmitting address request or registration messages on behalf of targeted victims to overflow their requester counters.

–Since there is no mutual authentication, it is well known that man in the middle attack is easily performed in the Diffie-Hellman Key Exchange scheme that the authors have adopted in their solution. The open wireless environment and multi-hop communications facilitate enormously this attack.

The centralized PAA simplifies the administration of autoconfiguration service, but it constitutes a weakness of security, especially when multiple PAA advertisement messages occur in one network or after network merges.

This problem has been treated by the authors who have proposed a solution to prevent a malicious node to become, in merge situation especially, the new PAA for the whole network. The proposal uses a validation process between merging networks PAAs. Their solution is too time-consuming preventing the protocol to operate quickly and correctly to detect merges. The security problems in this case and in the network initialization are left open.

3.6 Summary

By this analysis, we demonstrate that no solution suggested until now really solved the security problem for the IP address autoconfiguration service in MANETs. Table-2 summarizes the integrated mechanisms and weaknesses of the earlier proposals with respect to the attacks mentioned above. As an obvious result, the design of adequate secure and robust autoconfiguration schemes must meet quite considered requirements. The following section details these security requirements.

Table 2: Mechanisms and Weaknesses of previous autoconfiguration security schemes with regard to different attacks

	Proposal [11] Buiati et al.	Proposal [12] Cavalli and Orset	Proposal [13] Wang et al.	Proposal [14] Hu and Mitchell	Proposal [15] Langer and Kühnert
IP Spoofing Attack	vulnerable	vulnerable	vulnerable	vulnerable	vulnerable
Exhaustion Address Space Attack	vulnerable	vulnerable	-	-	vulnerable
Conflict Address Attack	vulnerable	vulnerable	vulnerable	-	vulnerable
False Conflict Address Attack	-	-	vulnerable	vulnerable	Protected
Sybil Attack	vulnerable	vulnerable	vulnerable	vulnerable	vulnerable
Traffic overload DoS Attack	vulnerable	vulnerable	vulnerable	vulnerable	vulnerable
Pre-authentication	YES, one way	Mutual	YES	NO	NO
Linked IP address	NO	NO	Hashed public key	NO	NO
Intrusion detection and accusation	YES	NO	NO	YES	YES
Consider network partition/merge	NO	NO	NO	NO	YES
Additional drawbacks	One-hop threshold based on-line Certification Authority	Threshold number of one-hop neighbors	Stateless scheme and lack of Certification Authority to sign generated public keys	Stateless scheme and many unrealistic assumptions	Stateless scheme, no message signature and Diffie Hellman key exchange problem

4. Requirements

In Mobile ad hoc networks, the required security level will depend on the context of deployment. Security mechanisms which will be implemented in military networks, for instance, are different from those of civil or commercial deployment. Resources of the mobile nodes and adversarial model are not obviously the same ones.
We consider here a strong and dynamic adversarial model. The imperative requirements for designing a secure and robust autoconfiguration scheme are as follows:

1. Nodes may enter or leave the MANET dynamically; the only requirement is that a node must hold a valid and unrevoked certificate. This supposes the existence of an Off-line Certification Authority for signing an 'Off-line Public Key Certificate' for any legitimate node that will participate in the MANET. To join the network, each node must hold its 'Off-line Public Key Certificate' and the public key of this Off-line Authority to be able to verify the validity of any 'Off-line Public Key Certificate'. If a node joins the network for the first time must use its 'Off-line Public Key Certificate' to be pre-authenticated.

2. Before any autoconfiguration, a mutual pre-authentication must take place between each IP address requester and the autoconfiguration server(s). The mechanism of mutual pre-authentication allows the servers to authenticate the requester, that is only legitimate nodes can take part in the network, but also the requester to authenticate the servers to prevent Man-In-the-Middle Attack.

3. Each node in the network needs to be able to verify at any time whether a public key is revoked, hence a revocation scheme is needed within the MANET. Nodes need to be able either to revoke their own public keys or to revoke the public keys of malicious/compromised nodes, which can be achieved by the so-called 'accusation schemes' [21].

4. The mechanisms set up to secure the address autoconfiguration service should not deteriorate the availability of the autoconfiguration service. At any given instant during the lifetime of the network, a new joining node should obtain with a secure protocol a unique IP address.

5. To avoid any single point of failure (trusted party), the autoconfiguration service must be initialized by a coalition of nodes instead of one node.

6. In order to manage the address space, the autoconfiguration scheme must be stateful. The IP addresses should be assigned exclusively by the network preventing malicious nodes to freely take part in the network.

7. The assigned IP address must be signed by an On-line Certification Authority. This allows a node to prove that its IP address has been assigned by the network.

8. The IP address must be bound to node's identity to counter the IP spoofing and Sybil Attacks. This seems to be the only reasonable solution to prevent these attacks. A certificate is commonly used for this purpose. According to requirement (7), this certificate must be signed by an On-line Certification Authority.

9. For any packets exchange, implied nodes must check if the originator's IP address corresponds to that appearing in its certificate, and if also this certificate is valid and unrevoked.

10. Finally, the scheme must take into consideration problems that may arise due to network partitions and merges.

5. Conclusion

MANETs are inherently characterized by open and hostile wireless environments, lack of infrastructure, dynamic topology and limited resources. When designing such networks, several interesting and difficult problems arise due to these characteristics. This has introduced new challenges including IP address autoconfiguration, routing, security and QoS, which have stimulated considerable research interest in recent years. In the context of security, there are still some unsolved problems such as bootstrapping security and autoconfiguration security issues. In this paper, we focused on the latter point. We have presented a survey and an analysis of all work related to this problem, highlighting theirs weaknesses, what led us to define the imperative security requirements overcoming earlier design faults. Our goal is to develop secure and robust protocols, which nicely fulfills the autoconfiguration task while thwarting all related possible attacks under rather strong adversarial model. Possible solutions to this issue will be considered in future work, exploiting recently published Discrete Logarithm based threshold cryptographic tools.

References

[1] C. Bernardos, M. Calderon and H. Moustafa, "Survey of IP address autoconfiguration mechanisms for MANETs", draft-bernardos-manet-autoconf-survey-03, April 2008.

[2] E. Baccelli (Ed.), "Address Autoconfiguration for MANET: Terminology and Problem Statement", draft-ietf-autoconf-statement-04, February 2008.

[3] H. Moustafa, C.Bernardos and M. Calderon, "Evaluation Considerations for IP Autoconfiguration Mechanisms in MANETs",draft-bernardos-autoconf-evaluation-considerations-03, November 2008

[4] K. Weniger and M. Zitterbart, "IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks", European Wireless 2002, Florence, Italy, Feb. 2002

[5] A. Misra, S. Das, A. McAuley, and S. K. Das. Sun. Autoconfiguration, Registration and Mobility Management for Pervasive Computing. IEEE Personal Communications, vol. 08, Issue 04, Aug. 2001.

[6] M. Mohsin and R. Prakash. IP Address Assignment in a Mobile Ad Hoc Network. IEEE Milcom 2002.

[7] H. Zhou, L. Ni, and M. Mutka, "Prophet Address Allocation for Large Scale MANETs", Proceedings of INFOCOM 2003, 2003

[8] Yuan Sun and Elizabeth M. Belding-Royer. A Study of Dynamic Addressing Techniques in Mobile Ad hoc Networks. Wireless Communications and Mobile Computing, vol.4, pp. 315-329, April 2004.

[9] Y. Sun and E. M. Belding-Royer, "Dynamic Address Configuration in Mobile Ad Hoc Networks," UCSB tech. rep. 2003-11, Santa Barbara, CA, Jun. 2003

[10] S. Nesargi and R. Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network", IEEE INFOCOM 2002, June 2002

[11] F. Buiati, R. S. Puttini, and R. T. de Sousa Jr., "A Secure Autoconfiguration Protocol for MANET Nodes". Lecture Notes in Computer Science, v. 3158, pp. 108-121, 2004.

[12] Ana Cavalli, Jean-Marie Orset, "Secure hosts autoconfiguration in mobile ad hoc networks" , ICDCSW.2004, pp. 809-814.

[13] Pan Wang, Douglas S. Reeves, Peng Ning, "Secure Address Autoconfiguration for Mobile Ad Hoc Networks", MOBIQUITOUS 2005. pp. 519-522.

[14] Shenglan Hu, Chris J. Mitchell, "Improving IP address autoconfiguration security in MANETs using trust modelling", Mobile Ad-hoc and Sensor Networks - First International Conference, MSN 2005, pp. 83-92.

[15] André Langer and Tom Kühnert, "Security issues in Address Autoconfiguration Protocols: An improved version of the Optimized Dynamic Address Configuration Protocol". archiv.tu-chemnitz.de, 2007

[16] C. Perkins, J. Malinen, R. Wakikawa, E. Belding-Royer, and Y. Sun, "IP Address Autoconfiguration for Ad Hoc Networks", draft-ietf-manetautoconf- 01.txt, November 2001

[17] J. Jeong, J. Park, H. Kim, H. Jeong, and D. Kim, "Ad Hoc IP Address Autoconfiguration," IETF Internet Draft, draft-jeong-adhoc-ip-addr-autoconf-06.txt. 2006

[18] Johnson, D.B., Maltz, D.A., Hu, Y.C.,"The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. (DSR)". 2004, IETF Draft: draft-ietf-manet-dsr-10.txt

[19] R. Puttini, L. Me, R. de Sousa, "MAE – MANET Authentication Extension for Securing Routing Protocols", 5th IEEE International Conference on Mobile and Wireless Communications Networks (MWCN2003), October 2003.

[20] K. Weniger, "PACMAN: Passive Autoconfiguration for Mobile Ad Hoc Networks," IEEE JSAC, Special Issue on Wireless Ad Hoc Networks, Mar. 2005.

[21] C. Crépeau and C.R. Davis. A Certificate Revocation Scheme for Wireless Ad Hoc Networks. Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), pp.54-61, 2003.

Abdelhafid Abdelmalek received the Laurea degree in Telecommunication Engineering from Institute of Telecommunications Oran (Algeria) in 1991, and Diploma of deepened studies in optoelectronic at Nancy (France) in 1993. From 1994 to 2000, he worked as engineer in charge of design and management of ISDN networks at Algerie Telecoms Company. In 2002, he received a Magister Diploma in Signals and systems at Tlemcen University, Algeria. From 2004, he is a PhD researcher. His research interests include data communications, Mobile networks, security, protocols and next generation networks.

Mohammed Feham received his Dr. Eng. degree in optical and microwave communication from the University of Limoges (France) in 1987, and his PhD in Science from the University of Tlemcen (Algeria) in 1996. Since 1987, he has been an Assistant Professor and Professor of microwave and communication engineering. He has served on the Scientific Council and other committees of the Electronics and Telecommunication Departments of the University of Tlemcen. His research interests include telecommunication systems and mobile networks and services.

Abdelmalik Taleb-Ahmed received a post graduate degree and a PhD in Electronics and Microwaves from the Université des Sciences et Technologies de Lille 1 in 1988 and 1992. From 1992 to 2004, He was an Associate Professor at the Université du Littoral Cote d'Opale de Calais. Since 2004, He is currently a Professor at the Université de Valenciennes et du Hainaut Cambrésis, and does his research at the LAMIH URM CNRS 8530, His research interests include signal and image processing.