Authentication, Authorization and Accounting (AAA) in Hybrid Ad hoc Hotspot's Environments

ABSTRACT

Wireless LAN (WLAN) is rapidly growing as a popular technology for ubiquitous communication, where Internet access is being a standard commodity. The growing demand in WLAN technological development is to provide high quality and secure Internet access to mobile users using their portable devices. Nevertheless, WLAN is still restrictive, as it requires the presence of mobile users in the communication range of access points. Moreover, the security of this network is posing a major challenge for its usage. Hybrid ad hoc networks appear as an attractive solution in public hotspots applications, allowing mobile users to achieve WLAN access independent of their existence in access points communication ranges. Since effective Authentication, Authorization and Accounting (AAA) are of great importance for secure mobile wireless access, in this paper we propose a novel architecture that provides efficient AAA and secure communication among mobile clients in WLAN hotspots applications. Our solution uses the hybrid ad hoc network concept and considers the service provider as the single point of contact for all AAA transactions. We adapt the IEEE 802.11i standard to the hybrid ad hoc network environment in order to set up authenticated links on layer 2, achieving secure wireless access as well as confidential data transfer. Since IEEE 802.11i necessitates the existence of a fixed infrastructure between the WLAN and the authentication server, we introduce a cross-layer interaction with the ad hoc routing layer in order to provide a virtual infrastructure among the mobile clients through employing a clustering mechanism. We validate our proposed solution through simulation. Through analyzing the obtained results, we give some performance estimates and we show the advantages of using the hybrid ad hoc networks approach.

Categories and Subject Descriptors

C.2.3 [Computer – Communication Networks]: Miscellaneous

General Terms

Management, Security, Standardization

Keywords

Wireless LAN, hybrid ad hoc networks, security, AAA, 802.11i.

1. INTRODUCTION

WLANs have emerged to fill the growing Internet demand. Through employing the WiFi technology, typically based on the IEEE 802.11 standard, a mobile user in the communication range of an access point is provided with Internet access. Access points (APs) are deployed at densely populated areas such as airports, railway stations and public hotspots, where the Internet access is heavily used. Although the WiFi technology offers high bit rate compared to cellular networks, it is still restrictive in terms of its limited coverage, requiring the existence of mobile nodes in the communication range of an AP in order to access WLAN services. Employing networks that provide high bit rate with broad coverage is taking a lot of attention from the research community and network operators. Hybrid ad hoc networks appear as an attractive solution in extending the service area of WLAN infrastructures, and are expected to offer seamless wireless network access for mobile users, avoiding the deployment of a huge number of APs. These networks employ a multi-hop access mode; combining pure ad hoc networks and fixed infrastructure. Each mobile node may access the fixed infrastructure either directly or via other nodes in a multi-hop fashion. In addition to having access to a fixed infrastructure, hybrid ad hoc networks may provide communication between mobile nodes, allowing peer to peer communication between users. There are several benefits for considering hybrid networks design. From an infrastructure point of view, there is no need to deploy new hardware, since wireless access points are becoming ubiquitous and almost all laptops and handheld devices are equipped with WiFi interfaces. Also, employing hybrid ad hoc networks is expected to satisfy mobile users’ needs via providing seamless mobility and Internet access. Furthermore, these networks are expected to reduce the number of APs needed to cover a crowded area and to reduce the impact of collisions with multiple users attached to the same AP. In fact, an important research and development aspect in hybrid ad hoc networks concerns the usage of standardized transmission systems like 802.11. Several ad hoc network functionalities and integration strategies are required for services’ delivery to users in such networks. Essential features like information routing, security, authentication, authorization and billing should be highly considered. The routing of information should be reliable and scalable, minimising resources’ consumption and delay. The security mechanisms must guarantee that only authorized users can use the network resources and access the services offered by the provider. Also, eavesdropping as well as modification of the transmitted data must be prevented. In this paper, we propose a novel architecture intended for hybrid ad hoc networks in public WLANs hotspots, with typically the Internet access as the potential service offered to mobile clients. An Authentication,
Authorization and Accounting (AAA) scheme is developed for convenient and secure communication between mobile users, authorizing only subscribed users to access the Internet service. Our proposed architecture adapts the 802.11i [1] to the hybrid ad hoc network environment, allowing extended forwarding capabilities in 802.11i without compromising its secure features. We introduce the concept of cross-layer interaction with the ad hoc routing layer in order to provide a virtual clustering infrastructure useful for the 802.11i operation. The remainder of this paper is organized as follows. We review the related work in Section 2. Section 3 gives the problem statement, highlighting the motivation to our work. Section 4 presents our proposed architecture and Section 5 gives a brief security analysis for our work. Our simulation results and performance analysis are presented in Section 6. We conclude the paper in Section 7.

2. RELATED WORK

The majority of research in hybrid ad hoc networks addresses routing techniques for such networks. The possibility of non-cooperative mode is also studied, aiming to save resources and bandwidth in such networks. Despite the fact that security is one of the major concerns in migrating to WLAN and the emergence of 802.11i to enhance the security margins of WLAN, only few contributions have treated the problem of security and access control in hybrid ad hoc environments. Jurca and Hubaux [2] highlighted the need of employing hybrid ad hoc networks to increase the coverage and the service zone of the 802.11i WLAN infrastructures. They have shown the advantages of such networks in reducing energy consumption of mobile nodes and allowing less interference. Ingelrest, Simplot-Ryl and Stojmenovic proposed several protocols for broadcasting and routing in such networks [3]. They also emphasized the idea of using hybrid routing protocols via applying proactive routing to maintain links to the closest AP and reactive routing between each two ad hoc nodes, where APs may cooperate in the later case to reduce the broadcasting overhead in the route discovery phase. Similarly Nilson, Garcia-Luna-Aceves and Spohn [4] proposed a novel hybrid routing approach that combines the proactive and reactive routing paradigms by relying on netmarks. They defined netmarks as nodes hosting special services to other nodes in the network (examples are DNS proxy nodes or AAA servers). Campos and Elias presented in [5] a simulation-based performance analysis of ad hoc routing protocols in a hybrid ad hoc network scenario. However, this study is restricted to establishing videophone session applications. Mitsianis [6] studied hybrid ad hoc networks for scenarios that do not necessitate cooperation between nodes. The author considers an opposite approach to treating selfish nodes in ad hoc network environment, aiming to conserve bandwidth and battery power. An incentive-based architecture is proposed offering a free-trade community in which mobile nodes can switch to non-cooperative mode when it does not worth relaying packets for others. The underlying trading protocol is based on a combination of public key and symmetric cryptographic primitives. Zhang and al. presented an AAA solution for mobile users in a WLAN hotspot application, integrating the AAA process and data transmission at the IP layer [7]. The authors used IPsec between APs and mobile terminals for per-packet authentication. Actually, this solution does not guarantee the secure links setup and is not totally transparent to hybrid ad hoc network environments. Also, an authentication scheme suitable for public wireless local area networks (PWLAN) was proposed by Yubo and Aiqun [8]. The main idea in this contribution is decreasing the functionalities on APs via employing access controllers (ACs). These ACs are charged with the network management and user authentication in order to reduce the complexity and cost of each individual AP. Still, this approach invokes the notion of centralized management devices without offering solutions to WLAN service extension and seamless Internet access. Finally, Shaer and al. [9] benefited from the 802.11i to extend the operational range of APs in a secure fashion. A framework is implemented to integrate secure node relays with APs emulation, aiming to provide secure handoff without compromising the secure features of IEEE 802.11i. Nevertheless, this approach is not transparent to the 802.11i operation and it involves new messages in a broadcast and multicast manner. From our investigation to the relevant contributions, we noticed that the problem of security in hybrid ad hoc networks is a young research domain showing only few contributions. The majority of the proposed contributions is restrictive and is not totally transparent to hybrid ad hoc networks. Until now, no efficient AAA scheme is proposed to offer secure links setup and confidential data transfer among mobile clients in a hybrid ad hoc network environments. In our work, we focus on providing an efficient AAA mechanism in hybrid ad hoc network environments, adapting the 802.11i to such network technology. We employ a cross-layer interaction with the routing layer in order to provide a virtual infrastructure that helps authentication and access control in such dynamic environments. Our approach considers the benefit of both mobile clients as well as network operators and is transparent to the 802.11i operation.

3. PROBLEM STATEMENT

The increasing business demand to offer Internet access services in a ubiquitous and a seamless manner increases the need for employing hybrid ad hoc networks to recover the existing limitations in the WLAN technology. Most deployments of public WLAN access solutions focus only on Internet connectivity, while employing hybrid ad hoc networks architecture is not enough considered. This is of great interest for network operators, and would require virtual infrastructures to extend WLAN service ranges. Also, this would require convergent and extensible Authentication, Authorization and Accounting (AAA) mechanisms. At the same time, hybrid ad hoc networks allow the satisfaction of service access for mobile clients with seamless mobility and confidential transfer. In this paper, we follow a realistic approach, which is beneficial to both mobile clients of WLAN hotspots and the network operator. We propose a novel architecture that provides an integrated solution. Our architecture considers a virtual infrastructure extending WLAN service ranges, mobile clients' seamless Internet access, and authentication and secure communication.

4. PROPOSED ARCHITECTURE

The general objective of this architecture is supporting mobile clients' secure and seamless access to the Internet, near public WLAN hotspots, even when they move beyond WLAN communication ranges. We assume that this architecture is provided by the network operator, utilizing its existing aggregation (backbone) network, and that the potential service provided is the wireless Internet access. Figure 1 illustrates the
architecture design overview. A hybrid ad hoc network that combines a fixed network infrastructure and a virtual infrastructure consisting of mobile clients is used. The fixed infrastructure has two core entities: a) the aggregation (backbone) network managed by the network operator forming the backend of the fixed infrastructure and providing Internet connectivity, and b) the WLAN 802.11 APs which implement the front end of the fixed infrastructure and are deployed at WLAN hotspots.

Each AP is linked to an existing ADSL broadband Internet access node. The virtual infrastructure (or the non-fixed infrastructure) is composed of mobile clients through ad hoc clusters constructed in a random fashion. Each chain of ad hoc clusters is linked to the infrastructure via an AP as shown in Figure 1. We used a cross-layer interaction with the ad hoc routing protocol in order to provide this clustering infrastructure. An efficient AAA mechanism is developed, adapting the 802.11i to the hybrid ad hoc hotspot's environment, providing efficient access control and achieving secure links setup.

4.1 Business Model

We consider commercial WLAN hotspots employing a paying access model. In order to ensure the proper operation under this model, the fulfillment of our proposed AAA mechanism is necessary. Actually, due to the transient nature of WLAN usage scenarios, it would be inconvenient for mobile clients to go through the payment process each time they use the WLAN. So, an on-use package (using pre-paid cards) model where payments are made according to the WLAN utilization is not so appropriate with our proposed architecture due to the difficulty of managing the accounting information for mobile clients. Such type of model should be complemented with appropriate mechanisms for efficient and appropriate accounting, which is out of the scope of our work. However, we propose a pure package (pay before use) business model, which is associated to the clients’ Internet subscription or telephone subscription and where the billing is monthly fixed whether the client uses the service or not. This model offers different privileges for clients according to their type of subscription, allowing the network operator/service provider to master the clients’ access.

4.2 Virtual Infrastructure through a Cross-Layer Interaction

Classical 802.11i depends on architectural elements in order to carry out the authentication process. It employs an authenticator (WLAN AP) and an authentication server as fixed elements; where mobile clients are the supplicants that request authentication from the authentication server via the authenticator. To achieve efficient AAA employing the 802.11i in our hybrid ad hoc hotspot environment, a virtual infrastructure is needed to provide a sort of centralization. This allows mobile clients to authenticate through special nodes dedicated to carry out the role of virtual authenticators. We benefit from the existing ad hoc routing, where the routing protocol is in charge of providing a dynamic routing infrastructure. We exploit a cross-layer interaction with the routing layer that enables each node in the network to evaluate its own status locally and to establish a network global view according to some defined metrics. Our goal is to provide a hierarchical clustering infrastructure among mobile clients representing the virtual infrastructure for the extended 802.11i operation.

4.2.1 Initial hypothesis and clusters’ classification

We consider the following hypothesis in providing the hierarchical clustering infrastructure, aiming to have a sort of centralization: each cluster has i) a fixed diameter equal to 1 hop, ii) a defined density for each cluster head (CH) determining the maximum number of nodes the CH can support, and iii) a defined depth for each CH, determining the possible number of its downstream clusters. The CH density reflects the capacity of links provision in the cluster and its value depends on the CH battery level, the CPU, memory and transmission power. Consequently, the CH depth is calculated as a function of the current CH density and its maximum density. In a first step, a default cluster is constructed around each AP by mobile clients falling in its communication range and authenticating directly through the AP via classical 802.11i. Since this type of clusters is privileged in term of lesser number of hops to reach the authentication server and access the Internet, we call this type of clusters primary clusters. In a second step, a number of ad hoc clusters are constructed in a random fashion among mobile clients that are out of the WLAN communication range. In this case, some mobile clients are selected to be CHs. Each CH plays the role of a friend node or an auxiliary authenticator for mobile clients belonging to its cluster. We call this type of clusters secondary clusters, since they are less stable with respect to primary clusters and they require more number of hops to reach the authentication server.

4.2.2 Routing protocol role in providing clusters

Since the CHs are the core critical entities in such a virtual infrastructure, a cross-layer interaction with the ad hoc routing protocol provides the necessary information for the choice of CHs. The following criteria are considered: i) CH density, ii) CH depth, and iii) stability of the CH node. If the secondary cluster is more than two hops from the access network, a trace of the upstream CHs depth is considered. To have an estimate on the CH stability, we use information of the CH actual position compared to its previous positions, saved as previous history beforehand. The routing protocol is responsible for the initial calculation and periodic updates of the density, depth, and stability of each node. Then it provides a downward feedback for this information to be stored at each node and to be used in the clustering construction. The routing protocol is also responsible for providing continuous downward feedback on each node state (CH or a cluster member, belonging to a primary or a secondary cluster). Based on this continuous information the virtual infrastructure is constructed...
and reconfigured in a dynamic manner, where clusters’ construction takes place respecting the following priorities:

- The first mobile client falling in the proximity of an AP associates with this AP constructing a primary cluster. The AP is considered as the CH and plays the role of the authenticator to all its cluster members.
- Secondary cluster construction takes place among mobile nodes that do not fall in the communication range of APs. Each node failing to associate with an AP starts to construct a secondary cluster through choosing a CH respectively considering the following priorities: a) CH belongs to a primary cluster and satisfies the previously mentioned conditions necessary for CHs; b) CH belongs to a secondary cluster and satisfies the criteria of choice of the CH.

The process of joining existing clusters takes place following the same priorities of clusters’ construction case. This approach is advantageous for network operators in the sense of mastering clients’ privileges according to their subscription. For example, gold clients would have the privilege to join the nearest clusters to the infrastructure or clusters of small density, so that to benefit from better connections.

4.3 Authentication, Authorization and Accounting (AAA) Mechanism

In this mechanism, the network operator is considered as the core of the AAA process. The IEEE 802.11i is adapted to the hybrid ad hoc hotspots’ environment via supporting extended forwarding capabilities, without compromising its secure features. We consider that the authentication server (AS) is a RADIUS server that resides in the access network of the operator (see Figure 1).

To accomplish the AAA process for a mobile client that exists in the WLAN communication range (proximity of 802.11 AP), the classical 802.11i authentication and messages’ exchange takes place. Each mobile client is the supplicant that initiates the authentication process. The 802.11 AP plays the role of the authenticator that authenticates the mobile client via contacting the RADIUS authentication server.

In the sequel we use MN to refer to a mobile client, authenticator to refer to the AP and AS to refer to the authentication server. EAPoL encapsulating EAP-TLS [10] is used between the MN and the authenticator, while RADIUS protocol [11] is used between the AP and the RADIUS server. Figure 2 illustrates the corresponding messages’ exchange in this case. To accomplish the AAA process for a mobile client that does not exist in the WLAN communication range (out of the proximity of an AP) and is consequently belonging to a ad hoc cluster, 802.11i is extended to support forwarding capabilities. In this case, we introduce the notion of friend nodes to allow each mobile client to initiate the authentication process through a selected node in its proximity.

The friend node plays the role of an auxiliary authenticator and forwards the authentication request of the MN to the actual authenticator AP. If the friend node does not fall in the communication range of the AP, it invokes other friend nodes in a recursive manner until reaching the AP. EAPoL encapsulating EAP-TLS is used between the MN and its direct friend node (auxiliary authenticator). For forwarding compatibility and secure messages’ exchange, we employ the notion of proxy RADIUS [13]. In such case, the selected friend node has a RADIUS client support relaying the authentication messages of the MN to the AP. The AP works as a RADIUS proxy, receiving RADIUS messages from the friend node and relaying them to the RADIUS server. Proxy chaining [13] takes place if the friend node is not directly connected with a WLAN AP. Figure 3, illustrates an example of the proxy chaining messages’ exchange.

As illustrated in Figure 2 and Figure 3, a Pairwise Master Key (PMK) is generated by the MN and by the AS to provide mutual authentication between each two communicating parties through involving the AS being a trusted third party. The PMK is derived from another initial key named Master Key (MK), which is a symmetric key between the MN and the AS. The AS transfers the PMK to the authenticator (AP) of the MN, then this key is transferred to the auxiliary authenticator(s) in case of employing RADIUS proxy chaining. At this phase, a secure channel access is provided between the MN and its authenticator (AP or friend...
node). In our AAA mechanism, we allow the storage of the PMK corresponding to each client authentication at the authenticator and auxiliary authenticators (if any). This allows fast roam back between mobile clients and APs having matching PMKs, with no need to authenticate from the beginning. Also, previously authenticated mobile clients sharing the same PMK can easily reauthenticate in a rapid mean. We call this scheme optimized reauthentication, where it appears useful in minimizing layer 2 delay in such a dynamic environment. In this context, the network operator privileges some mobile clients according to their type of subscription. Thus, PMK storage is associated with a certain time-stamp and is limited to a certain storage hierarchy according to the type of subscription. To obtain an increased security on each authenticated link, we introduce the 802.11i encryption phase that employs the Advanced Encryption Standard (AES). This takes place through the 4-way Handshake between the MN and its authenticator (AP or friend node).

Figure 4 illustrates the corresponding messages’ exchange using EAPoL-Key messages, allowing secret key information exchange.

Firstly, PMK is used to derive a Pairwise Temporal Key (PTK) for encrypting unicast data transfer on the link. Then, a Group Temporal Key (GTK) is derived for encrypting broadcast and multicast data transfer on the link. Thereby, all upcoming data transfer on the authenticated link will be encrypted using the generated keys ensuring communication privacy and secure data transfer. We utilize the same message structure used in RSN with reducing the number of handshakes messages via applying the WPA2 new key exchange messages [14]. This improves the time requirement and reduces the control overhead for mobility in the WLAN.

4.4 Required Implementation Consideration for Mobile Nodes

For appropriate implementation of the proposed architecture and correct functioning of our developed AAA mechanism, the AS should be involved at least once in order to authenticate each mobile client. This takes place either directly through the authenticator or through employing the concept of proxy chaining when mobile clients belong to secondary clusters. In addition, we require some characteristics for mobile clients including their support to some protocols. Table 1 illustrates these characteristics.

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Required Capabilities</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile client</td>
<td>Cluster Information Field</td>
<td>Storing a record of the node's status (CH or non CH, type of its cluster, density, depth including trace of upstream CHs depth)</td>
</tr>
<tr>
<td>GPS equipment</td>
<td>Acquiring Position Information</td>
<td></td>
</tr>
<tr>
<td>Mobile client or AP</td>
<td>Proxy RADIUS and/or Client RADIUS</td>
<td>Client RADIUS: Initiates the authentication messages transfer Proxy RADIUS: relays authentication messages between the client RADIUS and the authentication server</td>
</tr>
<tr>
<td>RADIUS server and proxy</td>
<td>Support the Microsoft Key delivery in the specific vendor attribute [16]</td>
<td>PairWise Master Key (PMK) transfer</td>
</tr>
</tbody>
</table>

5. SECURITY ANALYSIS

In our developed AAA mechanism, mobile clients are authenticated and authorized to access the Internet service in a manner that depends on their subscription type, allowing some clients to have privileged access. Employing the friend node concept allows mutual authentication and secure links’ setup between each communicating mobile clients. One of our major objectives is to impose the minimum possible AS solicitation in order to provide a better connectivity quality. Employing the PMK storage provides an optimized re-authentication between each associating pair having a matching PMK. This reduces the authentication delay and saves the overhead of involving the AS, thus allowing what is called fast roaming. The fact of caching authentication materials, contained in PMKs, in mobile nodes does not compromise the security due to the efficiency of the AES protocol and the time-stamp for each stored PMK managed by the network operator. However, we propose employing a mechanism responsible for PMK revocation among the nodes that leave the network. Thanks to the encryption key generation that follows the mutual authentication phase, our approach ensures confidential data transfer via encrypting data transfer on each link. Indeed, utilizing reduced number of handshakes messages saves latency and overhead. Although the end to end security is not always assured in the proxy RADIUS chaining due to the concept of secret sharing, our solution assures the end to end security with the proxy chaining as the proxy chaining takes place between the MN and the CH node who already have secured links between them.

6. PERFORMANCE ANALYSIS

We carried out a simulation-based performance analysis using Network Simulator2 (ns2) [17]. We choose to use a simulation-based approach due to the need to evaluate an integrated WLAN hotspot architecture employing a hybrid ad hoc network with an acceptable number of nodes. Our simulation considers the architecture deployment in terms of the 802.11 WLAN infrastructure as well as the authentication server, and we simulated the set of protocols used in our proposition. In the
MAC layer, we implemented the classical 802.11i as well as its extended capabilities on top of 802.11b. To correctly evaluate our proposed AAA mechanism, we implemented the RADIUS protocol together with EAPoL/EAP-TLS. Furthermore, we simulated a cross-layer interaction module with the routing protocol to benefit from layer 3 routing protocol in the virtual infrastructure construction. Our cross-layer interaction approach is quite general to be applied with any ad hoc routing protocol. Since a reactive routing approach fits well in our WLAN hotspot application, we simulated our cross-layer interaction module on top of Dynamic Source Routing (DSR) protocol [18]. This performance evaluation approach was not feasible to be done through implementation. However, as a next step we tend to carry out an implementation based evaluation for some critical scenarios based on our simulations results.

6.1 Experimentation Methodology
In our experiments, we validate our proposed architecture and analyze the extended 802.11i performance under a range of various mobility scenarios. All simulations have been run using a hybrid ad hoc network composed of 30 nodes moving over rectangular 1500 m x 500 m topography, and operating over 1200 seconds of simulation time. In our simulations we consider that the AS is residing at the architecture backend. We also consider that the WLAN APs show more reliability over mobile nodes, in having an unlimited amount of energy and a larger transmission range. The communication range of APs is configured to be 250 meter, while each mobile client is configured to have a communication range equal to 125 meter. We deployed the APs in an incremental fashion, from AP1 to AP5, in the centre of the topography. Thus we can estimate the impact of the lack of infrastructure as well as infrastructure availability on the behavior of mobile clients and on the protocols’ performance.

![Figure 5. Incremental WLAN infrastructure deployment.](image)

Figure 5 illustrates the incremental approach used in APs deployment, showing the WLAN communication range incremental coverage. We started by a limited WLAN infrastructure deploying AP1 in the centre of the topography, covering only Area1 of the topography. Then we sequentially deployed AP2 on the left hand side of AP1, adding Area2 to the WLAN coverage and AP3 on the right hand side of AP1, adding Area3 to the WLAN coverage. At this phase, the WLAN provides a full coverage for the topography. As a next step, we introduced an overlapping between the APs communication ranges through sequentially deploying AP4 and AP5, providing respectively Area4 and Area5 coverage. The simulated virtual infrastructure includes ad hoc clusters constituted in a random fashion extending the coverage of the WLAN infrastructure. The movement pattern of mobile clients is totally random, to confirm with a real hotspot application, with maximum speed equal to 1.1 m/s. To achieve this, we used the Random WayPoint (RWP) mobility model [19] with pause time equal to 0. In our simulation, each mobile client N initially authenticates at time T0, where T0 is a random variable uniformly distributed over the interval [0,50] seconds. In case of authentication failures or the need to authenticate to new authenticators and/or auxiliary authenticators while moving, authentication trials take place at time T0, which is a random variable uniformly distributed over smaller intervals. We carried out our experiences considering two cases: WLAN APs with no ad hoc clustering extension and WLAN APs with ad hoc clustering extension. In each studied case, we ran our simulations once with no optimized re-authentication and once with optimized re-authentication. Our performance evaluation is a result of 400 different simulations, using 20 different simulations for each studied case. As we do not focus on analyzing the impact of the application layer traffic, we used CBR traffic with light load on the network.

6.2 Results and Analysis
During our analysis, we firstly studied the performance of WLAN APs with no ad hoc clustering extension (denoted in the sequel by non clustering case), and with ad hoc clustering extension (denoted in the sequel by clustering case). Secondly, we studied the gain of the optimized re-authentication in the clustering case. Finally, we studied the effect of the ad hoc chaining on the performance of the authentication process in the clustering case.

We assume that mobile clients should firstly authenticate in order to setup links on layer 2 and to consequently obtain Internet access service. Thus, successful authentication is a necessary condition for successful service access. We derived the following performance metrics to study the effect of extending the 802.11i on the performance of the authentication process: i) average authentication delay: calculated as (Σ time required for each authentication) / (total number of authentications). The time required for each authentication includes all the messages exchanged between the authentication start and the authentication end. This time is represented by T4 in Figure 2, considering the classical 802.11i exchange. For extended 802.11i, the extra messages between proxies are included. ii) authentication failures: defined as the number of non-authenticated nodes, which are the mobile clients that failed to authenticate during the whole simulation time. iii) re-authentication optimization: defined as the number of re-authentications taking place without involving the main authentication server. iv) average authentication trials failure: calculated as (Σ number of authentication requests that are initiated by each mobile node and that did not succeed at authenticating the node) / (number of mobile nodes trying to authenticate). v) ad hoc clustering size: defined as the average number of ad hoc clusters constituted during the simulation time. vi) ad hoc chaining depth: defined as the ad hoc clusters hierarchy levels. vii) server solicitation ratio: calculated as (total number of authentication requests on the servers)/ (total number of authentications). viii) server request distribution: defined as the number of authentication requests on the server, per minute, during the simulation time. The values of these metrics
obtained from our simulation, per studied case, are average values resulting from running all our experiences.

In Figure 6 we study the clustering case versus the non clustering case. The obtained results for both cases are analyzed with different APs deployment in an incremental fashion to show the impact of the WLAN infrastructure size on each case. Figure 6(a) shows the average authentication delay in msec for the different APs configuration. We notice that the clustering case has higher average authentication delay compared to the non clustering case when the number of APs is small. This delay decreases gradually with the increase in APs deployment, where the two cases show nearly the same average authentication delay when the number of APs sufficiently covers the topography. Actually, the lack of APs coverage allows the construction of more ad hoc clustering hierarchy levels in order to authenticate far away nodes, resulting in more number of hops through the proxies in order to reach the AS and thus causing more delay. However, this delay difference is not harmful with a maximum difference of 20% compared to the non clustering case. On the other hand, with sufficient APs coverage, nodes prefer to authenticate directly via the existing APs instead of selecting friend nodes. This results in reducing the ad hoc clustering construction and hence reducing the delay.

Figure 6(b) illustrates the authentication failures, in term of number of the non authenticated nodes, for different configurations of APs. We can notice the advent of the clustering case in minimizing the authentication failures, especially when the number of APs does not provide enough coverage for the whole topography. We observe that the authentication failures reaches zero when the number of deployed APs start to provide sufficient coverage for the whole topography, resulting in equal effect for the clustering and the non clustering cases. In Figure 6(c), we study the effect of the optimized re-authentication on the behavior of the server solicitation ratio in the clustering and the non clustering cases with different APs configuration. The x-axis represents the number of deployed APs, the left y-axis represents the server solicitation ratio and the right y-axis represents the optimized re-authentication. Generally, we notice more server solicitation ratio for the non clustering case. This returns to the fact of the few occurrence of optimized re-authentication in the non clustering case. This is not clearly shown on the curve, due to the scale difference, but the average number of optimized re-authentication is less than 1. The low occurrence of optimized re-authentication is due to the distribution of nodes' authentication among only WLAN APs which only permits re-authentication of type "fast roam back". Consequently, the AS is solicited at nearly each authentication. On the other hand, there is a noticeable optimized re-authentication in the clustering case, especially with few APs deployment, which results in a noticeable decrease in the server solicitation ratio compared to the non clustering case. However, with the increase in the number of APs, we observe a decrease in the optimized re-authentication in the clustering case accompanied by an increase in the server solicitation ratio. This is due to the sufficient APs coverage affecting the nodes' authentication behavior, where they prefer direct authentication via APs and thus minimizing the possibility of re-authentication among friend nodes.

Figure 6. Studying clustering versus non clustering cases.

Figure 6(a). Average authentication delay.

Figure 6(b). Authentication failures.

Figure 6(c). Effect of re-authentication optimization on server solicitation ratio.

Figure 7(a). Average authentication delay.

Figure 7(b). Server solicitation ratio.
In Figure 7, we study the gain of the re-authentication optimization in the clustering case, taking into consideration the incremental deployment of APs. Figure 7(a) illustrates the average authentication delay in msec for different APs deployment for the cases of optimized and non optimized re-authentication. A noticeable delay difference is shown in the figure, where the non optimized re-authentication case causes more delay for all APs deployment. This is due to the increase in the AS solicitation in the non optimized case, where the AS is solicited each time an authentication takes place. In addition, there is an increase in the number of exchanged messages that are required for each authentication process. The delay difference decreases with the increase in the number of APs, and this difference disappears for the two cases when there is a sufficient AP coverage for the whole topography. Actually, when the number of APs increases, especially when the APs sufficiently cover the topography, the optimized re-authentication lacks its advantage as nodes are scattered among all existing APs allowing only "fast roam back" re-authentication that does not frequently occur among the large number of APs. In Figure 7(b), we study the server solicitation ratio in the clustering case in optimized and non optimized re-authentication cases with all APs deployment. Generally, more server solicitation ratio is noticed in the non optimized re-authentication for all APs configuration. This confirms the increase in the average authentication delay in Figure 7(a) in the non optimized re-authentication case, where more AS solicitation and messages exchange take place in this case. In the optimized re-authentication case, less server solicitation ratio is shown due to the lesser AS solicitation. However, when the number of APs increases, the server solicitation ratio starts to increase in the optimized re-authentication case, since the optimization in terms of re-authentication has lesser effect in this case. In Figure 7(c), we study the average authentication trials failure for optimized and non optimized re-authentication with different APs deployment. The x-axis represents the number of APs, the left y-axis represents the average authentication trials failure for authenticated nodes and the right y-axis represents the average authentication trials failure for non authenticated nodes. We analyzed the trials failure of nodes that succeed to authenticate (even after a number of trials) and the trials failure of nodes that did not succeed at all to authenticate (non authenticated nodes). A general notice is that the trials failure of authenticated and non authenticated nodes decrease with the increase in the number of APs in case of optimized as well as non optimized re-authentication. This is a logical behavior as the increase in the number of APs gives more chances for the nodes to reach the AS. Authenticated nodes show lesser trials failure in the optimized re-authentication case compared to the non optimized re-authentication case, since optimized re-authentication allows the re-authentication requests to be directly treated by friend nodes saving the trials failure if the AS is not reached or if there is a problem in the channel access preventing the re-authentication request transmission. With the increase in the number of APs, authenticated nodes show nearly equal trials failure in optimized and non optimized re-authentication cases. This is due to the smaller impact of the optimized re-authentication process with the increase in the number of APs. On the other hand, non authenticated nodes show nearly the same trials failure behavior, when the number of APs is small, for optimized and non optimized re-authentication cases. With the increase in the number of APs, the non authenticated nodes trials failure decreases gradually then settles at 0. In fact, thanks to the sufficient APs coverage, all the nodes succeed to authenticate as illustrated in Figure 6(b). Consequently, there are no more non authenticated nodes, implying no more trials and thus translating the 0 value of the authentication trials failure.

In Figure 8, we study the effect of the ad hoc chaining in the clustering case with optimized re-authentication consideration. Figure 8(a) illustrates the effect of the ad hoc chaining depth on the average authentication delay in msec. It is noticed that the more the ad hoc chaining depth the more the average delay. This is due to the increase in the number of hops and the
increased messages exchange, through proxies, to reach the AS. Also, we observe the ad hoc chaining depth decrease with the increase in the number of APs. As we previously mentioned, the APs higher coverage reduces the ad hoc clustering construction, allowing this shown decrease in the ad hoc chaining depth. Figure 8(b) illustrates the effect of the ad hoc clustering size on the authentication failures with different APs deployment. The x-axis represents the number of deployed APs, the left y-axis represents the ad hoc clustering size and the right y-axis represents the authentication failures. Firstly, it is noticed that the ad hoc clustering size decreases with the increase in the number of APs due to the smaller possibility of ad hoc clustering construction, when the APs start to sufficiently cover the topography. The maximum number of authentication failures takes place in case of 1 AP deployment, which is due to the difficulty of ad hoc clustering to provide full coverage for all nodes with this minimum infrastructure. However, a little increase in the number of APs allows more utilization of ad hoc chaining and thus allows less authentication failures. Then, when the number of APs start to sufficiently cover the topography, authentication failures is settled to 0.

Figure 9. Server request distribution.

In Figure 9, we study the server request distribution along the whole simulation time. We have chosen two deployment cases of APs (2 APs and 5 APs), in order to study the behavior of intermediate and sufficient coverage of infrastructure. We analyze the server request distribution for both optimized and non optimized re-authentication in the clustering case. A general notice for all cases is that the highest interval for server requests is at the first minute of the simulation time. Then, the interval of [2,8] minutes shows about 80% lesser server requests. Afterwards, a quite decrease in server requests is noticed until the end of the simulation, implying decreased server's activity. We observe that the 5 APs case shows more server requests, along the whole simulation time, compared to the 2 APs case. This is due to the lack or minimization of ad hoc clustering construction, reducing or masking the effect of the optimized re-authentication and causing more server solicitation. It is also noticed that the 5 APs case shows nearly the same server distribution for optimized and non optimized re-authentication cases, confirming the previous analysis. On the other hand, in the 2 APs case the optimized and non optimized re-authentication show nearly the same server distribution in the first interval, [0,1], of the simulation time. This is due to the initialization phase, when all nodes start to authenticate and the optimized re-authentication does not yet take place. Afterwards, along the simulation time, we observe that the 2 APs case shows lesser server requests with optimized re-authentication compared to non optimized re-authentication.

7. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a novel architecture for wireless Internet access in WLAN hotspots areas. We presented a hybrid ad hoc network solution that allows mobile clients outside the WLAN communication range to have secure Internet access. A major contribution of our architecture is providing each mobile client with secure communication and confidential data transfer while maintaining the wireless seamless Internet access. Those two aspects are two essential pillars for future business opportunities. To achieve this, we developed a new Authentication, Authorization and Accounting (AAA) scheme that supports public WLAN hotspots applications in hybrid ad hoc network environments. We also extended the 802.11i standard to such network environment via employing forwarding capabilities without compromising the security features in 802.11i. Our approach in adapting 802.11i to this dynamic environment is based on providing a virtual infrastructure among the mobile clients. The introduced cross-layer interaction with the ad hoc routing layer benefits from the ad hoc routing protocol in the construction of a hierarchical clustering infrastructure among mobile clients. As a result, efficient AAA process as well as secure links' setup takes place for each mobile client during the Internet access service. To validate out contribution, we carried out a simulation based performance analysis using ns-2, implementing our proposed hybrid ad hoc networking architecture together with our newly developed AAA mechanism. Our obtained results illustrate the advantages of introducing the virtual clustering architecture among the mobile nodes. From our performance analysis, we observed that the clustering approach can compensate the lack of APs (insufficient size of WLAN infrastructure) allowing secure service access for non covered nodes. In order to get a remarkable benefit from employing a hybrid ad hoc network, a tradeoff should be fulfilled between the size of the deployed WLAN infrastructure and the proper functioning of the ad hoc clustering offering a virtual infrastructure. We observed from our results the effect of the optimized re-authentication in minimizing the server solicitation ratio and the impact of the supplementary infrastructure deployment in loosing or masking the advantage of the optimized re-authentication.

For future work, we tend to analyze the performance of our proposition with different network sizes, different traffic types and different networks load. Also, a short term perspective is to implement this proposition for a selected scenario.

8. ACKNOWLEDGMENTS

Many thanks go to Frederic Jacq for our fruitful discussions on the EAP and RADIUS. We are also so thankful to Tinku Mohamed Rasheed for his useful notices concerning the clustering. This work was supported by France Telecom R&D SPONTEX project.
9. REFERENCES