On the Performance of Service Publishing in IEEE 802.11 Multi-access Environment

Dario Di Sorte, Mauro Femminella, and Gianluca Reali

***Abstract* — In a multi-access/service IEEE 802.11 environment, the problem of providing users with service-related information to support a correct and fast network selection is expected to become a very important issue. We present a quantitative comparison between the legacy scenario, where each user must enter a network point of access to check its service offer, and the enhanced scenario where some service-related information is broadcasted through beacons. Results confirm the effectiveness of the beacon-based approach, in terms of discovery time, server load, and bandwidth consumption.**

***Index Terms* — Service discovery, network selection, costs and benefits.**

I. Introduction

With the continuous increase of the number of IEEE 802.11 wireless accesses and services, the problem of network selection is expected to become a very important issue. Users may want to select the Access Point (AP) according to a number of factors beyond the signal strength (e.g., roaming agreements, security, QoS, supported services, price). For this reason, there is a strong need to develop a mechanism which allows a Mobile Terminal (MT), and thus a user, to access a larger amount of information before authentication/association with the AP in order to make the selection process more efficient (i.e., less time and bandwidth consuming). This need is extremely urgent in case of simultaneous availability of many APs in a given area, each with a different service offer. On the operator side, they may like to advertise their own services to both attract customers and minimize traffic load due to the failed attempts of users to find a specific service.

Some solutions on this subject have been proposed by the IEEE Task Group 802.11u, [1]. A viable one is to include additional service-related information within the beacons periodically broadcasted by APs (every 100 ms). They consist of variable-length mandatory and optional frame body components (Information Elements, IEs) [2]. This mechanism allows MTs to discover not only APs, but also certain service capabilities. To receive IEs which are not carried in beacons, a Probe Request/Response mechanism can also be used. Thus, to enhance the IEEE 802.11 standard, new IEs containing service-related information should be defined.

The goal of this manuscript is to show benefits and costs of the beacon-based service publishing solution in a multi-service/access 802.11 environment. We do not deal with all the issues related to information coding and standardization. We simply assume that users are allowed to access some service-related information before entering a given network.

The reference scenario is depicted in Fig. 1. Multiple accesses in the same area can be provided through either a number of APs or a Virtual AP (VAP). A VAP is a physical AP in which some logical entities, named VAP profiles, exist and operate on the same frequency [3]. From the user side, each VAP profile appears as an independent, physical AP. It represents an instantiation of a complete 802.11 MAC including BSSID, SSID, and capability set. A wireless network provider could differentiate the offered services within the same physical device, or different providers can share it and avoid frequency interference, which is typical of multi-AP deployment. In addition, VAP technology enables traffic isolation (e.g., VLANs, VPNs) to be extended to the wireless network. Hereafter we denote as AP both a physical AP and a VAP profile.

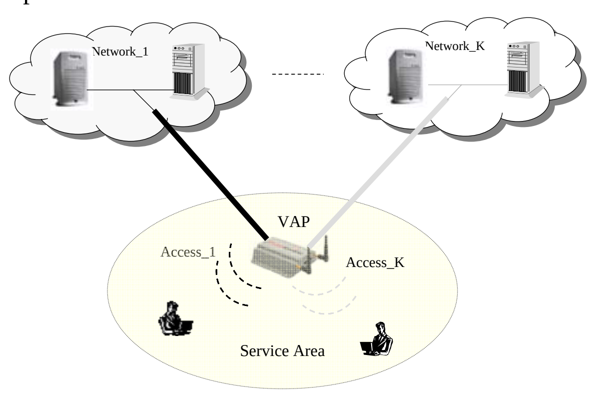

Fig. 1 – Network scenario.

II. Beacon-based Service Publishing

As illustrated above, we assume that some service-related information may be included within beacons. Clearly, this information should be limited so as not to cram beacons and consume excessive bandwidth. In order to allow users to perform a *preliminary* screening of the service peculiarities, beacons should include some “rough” information. Then, once the MT has associated with the target AP, a service discovery protocol may be used for obtaining more refined service attributes and configuration information. For instance, users may obtain additional information from an authentication server, a web server, a Service Location Protocol server, or a DHCP server. In general, we can assume that there is an Information Server (IS) able to provide users with the service attributes. Thus, for some kind of services, a user may realize if

This work was performed under co-financing by the MIUR within the project PRIN-TWELVE. The Authors are with Dipartimento di Ingegneria Elettronica e dell’Informazione (DIEI), University of Perugia, via G. Duranti 93, 06125 Perugia, Italy (e-mail: {disorte,femminella,reali}@diei.unipg.it).

the selected access can provide him/her with the desired service only after an IS query. For instance, if a user is looking for high definition color printing service, the access selection is based on a sketchy information within beacons, such as "printing service available". Then, the user may discover if the service with the desired attribute (*color* and *available definitions* printing) is available. Clearly, in other cases, the information included within beacons may be enough to execute a correct access selection.

We consider the presence of K APs in the reference area. The service discovery process is depicted by the flow diagram shown in Fig. 2. G is defined as the number of candidate APs from the network scanning process. In the legacy system $G=K$, whereas, in the beacon-based one, $G=W\leq K$, where W is the number of APs publishing sketchy information about the desired service.

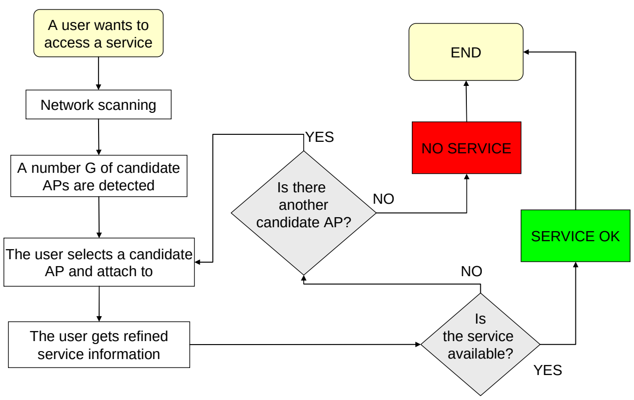

Fig. 2 – Service discovery process: flow diagram.

II.A Performance Evaluation

In this sub-section we evaluate some performance figures: (i) the average number of user attempts to obtain a specific service; (ii) the probability that an IS is queried; (iii) the wireless bandwidth consumption of both the beacon-based and the legacy approach to complete the service discovery process. We assume that:

– users have credentials to access all APs;
– each AP is associated with an IS;
– users are unaware of the available services in advance;
– the selection is uniformly distributed among candidate APs;
– users' behavior is mutually independent.

Under these assumptions, the probability that a service is found at the i-th attempt is:

$$P_i = \begin{cases} \dfrac{M}{G-i+1}\displaystyle\prod_{j=1}^{i-1}\left(1-\dfrac{M}{G-j+1}\right) & 1\leq i\leq G-M+1 \\ 0 & \text{otherwise} \end{cases}, \quad (1)$$

where M is the number of APs delivering the specific service. Thus, the average number of attempts for receiving this service is:

$$N=\sum_{i=1}^{G-M+1} i\cdot P_i\,. \quad (2)$$

Now we consider the IS standpoint. The probability of being contacted upon a service request is equal to:

$$P_{IS}=G/K\left(P_{S,OK}\cdot P_{C,OK}+\left(1-P_{S,OK}\right)P_{C,NO}\right), \quad (3)$$

where $P_{S,OK}=M/G$ is the probability that the specific service is provided through the selected AP, $P_{C,OK}=1/M$ is the probability that an IS is contacted to obtain information about an available service. Finally, $P_{C,NO}$ is the probability that an IS is contacted for a service not provided. It is easy to prove that:

$$P_{C,NO}=\sum_{j=2}^{G-M+1} P_j\,(j-1)/(G-M)\,. \quad (4)$$

Finally, let us evaluate the wireless bandwidth consumption of the beacon-based solution. It consists of two components. The former, L_{IE}, is the cost to include additional information within beacons; such a value is constant with the service demand. The latter, L_{User}, is the signaling cost associated with traffic exchange upon a service request and is equal to

$$L_{User}=\lambda\cdot D\cdot N\,, \quad (5)$$

where λ is the service request average arrival rate, $N=N_{Beacon}$ is the average number of user attempts to obtain the desired service given by (2) with $G=W$, and D is the average amount of signaling traffic to be exchanged for each attempt, which includes authentication, DHCP, and service discovery traffic.

The bandwidth consumption of the legacy system is given by (5), where $N=N_{Legacy}$ is provided by (2) with $G=K$.

To sum up, the wireless bandwidth saving of the beacon-based approach with respect to the legacy system is equal to

$$\Delta L=\lambda\cdot D\cdot(N_{Legacy}-N_{Beacon})-L_{IE}\,. \quad (6)$$

II.B Numerical Results

Fig. 3 shows the average number of user attempts (given by (2)) in both legacy (N_{Legacy}) and enhanced system (N_{Beacon}) versus the number of APs, W, which publish the service. The number of APs, M, which provide the specific service is set as a parameter; the number of APs in the surrounding area is equal to K=7.

The following considerations apply. As expected, the number of user attempts of the legacy system is independent of W; also, both N_{Legacy} and N_{Beacon} decreases with M. The number of attempts is definitely lower for the beacon-based system, and the gain decreases with W, for each value of the parameter M. When $W=K$=7, the performance of the two systems is clearly equivalent, since all the APs are candidates for a user access. The gain is maximized when $W=M$, i.e., when the APs which publish sketchy information on a service also provide the desired service. The gain increases when the values of both $W=M$ and N_{Beacon} decrease. When $W=M=K$, both the legacy and the enhanced system maximize the performance and one access attempt is sufficient to find the service.

In summary, when some different accesses provide different services, the beacon-based solution reduces the average number of user attempts to find a specific service. Note that the time needed to authenticate and associate with an AP, configure network parameters (via DHCP), and retrieve service-related information is dependent on the specific authentication and service discovery protocol and is typically of the order of some tens of seconds. Thus, the beacon-based solution guarantees a remarkable time saving when (K-M) is high; such a saving becomes even higher when (W-M) is low.

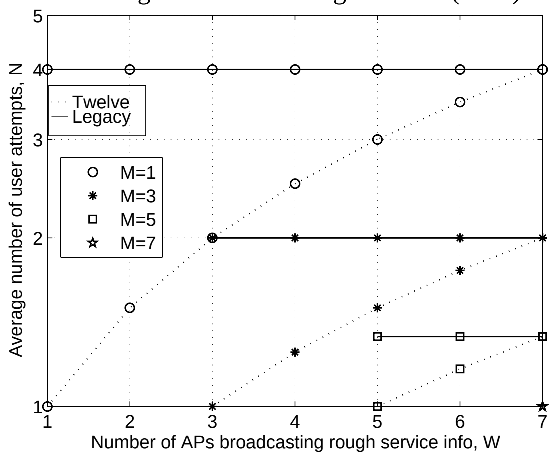

Fig. 3 – N_{Legacy} and N_{Beacon} versus W, with M as a parameter and K=7.

Fig. 4 shows the probability of an IS to be contacted (given by (3)) in both legacy ($P_{IS,Legacy}$) and enhanced system ($P_{IS,Beacon}$) versus the number of APs, W, which publishes the service, with the number of APs, M, which provides the specific service as a parameter; K is set to 7. As expected, curves have a shape similar to the ones of Fig. 3. $P_{IS,Legacy}$ is constant with W and decreases with M, whereas $P_{IS,Beacon}$ increases with W and decreases with M. To sum up, the beacon-based solution definitely reduces the load on the IS and in general on all the servers involved in the user access procedure (DHCP server, authentication server).

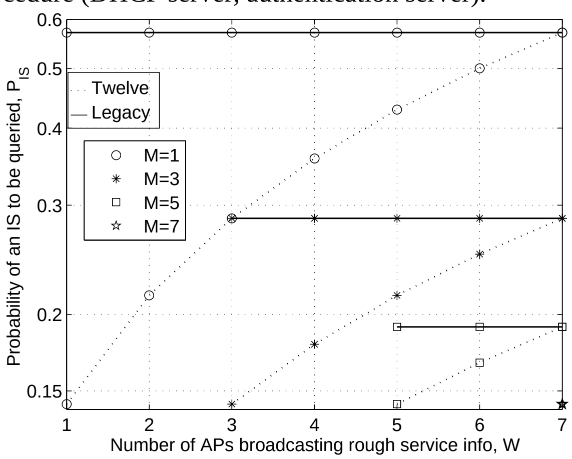

Fig. 4 – $P_{IS,Legacy}$ and $P_{IS,Beacon}$ versus W, with M as a parameter and K=7.

As regards the cost, L_{IE}, of sending additional service-related information within beacons, we have measured experimentally the wireless bandwidth consumption when the size of the beacon is changed. To this end, we have simply changed the length of the SSID (from 8 bytes to the maximum value equal to 32 bytes). We have loaded the network with UDP traffic at 11 Mbps and measured the throughput in downlink direction. The wireless access has been provided by the CN3200 VAP [4]; this has allowed us varying the number of VAP profiles, K, from 1 to 10. Note that we are considering the worst case, when all the accesses are on the same frequency. The measurement results are reported in Table I.

Table I – Wireless bandwidth cost versus *K*.

	K=1	*K*=4	*K*=7	*K*=10
L_{IE} (Kbit/s)	8.25	57.5	110	117.25

L_{IE}, as expected, increases with the number of profiles, since the number of beacons broadcasted increases and the effect of their enlarged dimension increases as well. Thus, we can conclude that the cost of the service publishing based on beacon management frames is negligible for traditional (single profile) AP and is also small when the number of active profiles (if the VAP technology is used) is low.

Fig. 5 shows the bandwidth saving on the wireless medium, ΔL (given by (6)), versus the offered load, λ, with the data load per-access, D, and the number of accesses, K, as parameters. We consider the case when only one access provides the service (W=M=1). Values of D ranging between 100 and 300 Kbytes are typical of an access providing web-based authentication, DHCP configuration, and web-based service information retrieval. As expected, the bandwidth saving increases with the number of surrounding accesses, K, the amount of traffic per access, D, and the service demand.

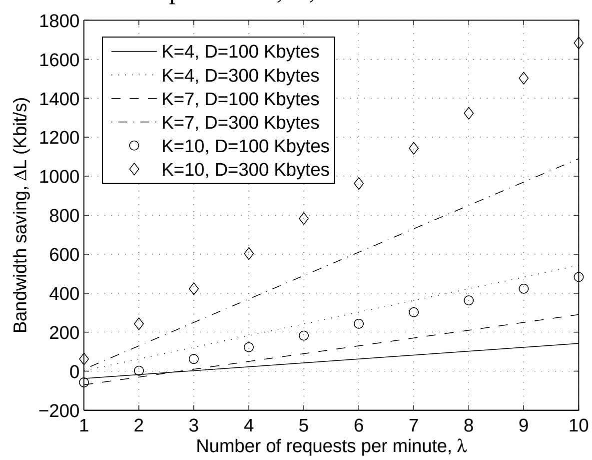

Fig. 5 – ΔL versus λ, with K and D as parameters and W=M=1.

III. Conclusion

In this letter, we have evaluated some costs and benefits of the beacon-based service publishing approach in an 802.11 multi service/access scenario. The analysis has confirmed the effectiveness of such a solution in terms of service discovery time, server load and signaling burden.

References

[1] http://grouper.ieee.org/groups/802/11/Reports/tgu_update.htm, IEEE 802.11, TASK GROUP U.

[2] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, 1999.

[3] Virtual AP Technology Multiplies WLAN Services, Whitepaper, Colubris Networks, March, 2004, available at http://www.colubris.com/downloads/whitepapers/wp_vap.pdf.

[4] The Colubris Web Site, MultiService Controllers, http://www.colubris.com/downloads/datasheets/DS_MSC_3000.pdf.