Information Embedding in IEEE 802.11 Beacon Frame

Vishal Gupta
Birla Institute of Technology and Science
Pilani, India

Mukesh Kumar Rohil
Birla Institute of Technology and Science
Pilani, India

ABSTRACT
According to IEEE 802.11 protocol, beacon frames are periodically transmitted by the Access Point (AP) and carry mostly network specific information. All the wireless stations (or wireless clients) with in the "vicinity" of transmission range of AP receive corresponding beacon and use the information embedded in it for various purposes. The arrangement of information in beacon is standardized by 802.11, thus facilitating communication between different devices manufactured by different vendors. Also, the IEEE 802.11-2007 is the base protocol and its several amendments have been published by IEEE till date. In this paper we show that with out breaching the standard, where additional non-standard information can be embedded on the transmitted fields of 802.11 beacon frame. This facilitates the non-standard, vendor/network specific communication of information from AP to wireless clients without Association.

General Terms
Wireless Communication, Wi Fi Network Architecture.

Keywords
Beacon stuffing, 802.11 beacon frame, Standardization.

1. INTRODUCTION
Just as Ethernet is dominant when it comes to LAN (Local Area Network) technologies, TCP/IP protocol suite is dominant when it comes to modern internetworking, IEEE 802.11 dominates the wireless LAN world. It not only attempts to model wireless networks as a replacement for wired networks, but because of its complementary characteristics to cellular networks it has emerged as one of the most prominent choice of cellular operators for mobile data offloading [1]. It provides the basis for wireless network products using the Wi-Fi brand.

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in 5, 3.6, and 2.4 GHz frequency bands. It is somewhat similar to a cellular architecture where the system is subdivided into cells, where each cell (called Basic Service Set or BSS in 802.11 nomenclature) is controlled by a AP. Over the past five years, IEEE LAN/MAN standards committee (IEEE 802) has published several amendments to the base IEEE 802.11-2007 protocol [9]. More specifically, it has undergone ten amendments: 802.11k-2008 [10], 802.11r-2008 [11], 802.11y-2008 [12], 802.11w-2009 [13], 802.11n-2009 [14], 802.11p-2010 [15], 802.11z-2010 [16], 802.11v-2011 [17], 802.11u-2011 [18], and 802.11s-2011 [19] respectively. Each amendment extends the functionality of the previous one, thus extending the scope of 802.11. For example, the ninth amendment, 802.11u, supports interworking of 802.11 network with external networks, thus facilitating the globalization of cellular - WLAN interworking.

If a wireless client needs to communicate using 802.11 network, it first listens to the beacon frame. This beacon frame is periodically broadcast by the AP and contains the necessary and basic information about the network. If the station decides to communicate with a particular AP (as there can be multiple beacons from multiple APs in the vicinity), it attempts Association. This decision to attempt Association with a particular AP is heavily based on the parameters standardized by the protocol and are present in various fields of the beacon. Once Association is successful then only the communication can start.

Often it is a requirement that non-standard vendor/network specific information is to be embedded in the beacon frame. Moreover, this information is to be embedded without breaching the standard because changing the standard according to the application needs will have multiple adverse effects on the proper and effective communication with other 802.11 devices. In this paper we show that where to embed more information in the transmitted fields of IEEE 802.11-2007 beacon frame.

The scope of our work is limited to the following:

a) The ideas and results presented are valid up to the IEEE 802.11 -2007 base standard. Moreover, it is assumed that AP beacon interval is 10 ms. In fact, this is configurable and can be different for different 802.11 networks.

b) The main aim of this paper is to propose that on the transmitted data of beacon frame some additional information can be embedded without breaking the standard and, in fact sometimes without increasing the size of beacon also. The implementation will depend on the application and information to be embedded.

The rest of the paper is organized as follows. Section 2 explains the applications of embedding additional information in the beacon frame. Section 3 explains the general frame format of beacon frame as per IEEE 802.11-2007 standard. Section 4 explains about various potential fields as given by R. Chandra et al [21] where additional information can be embedded. Section 5 discusses about the additional field which can be used to carry additional information. Section 6 discusses about the implementation of the scheme. Section 7 guides to some future work and possible extensions to this paper, and section 8 concludes the paper.

2. WHY ADDITIONAL INFORMATION IN BEACON?

There are numerous potential application areas which requires embedding additional information in the beacon frame. One of its major application is in Network Selection in heterogeneous networks (like that of 3G-WLAN interworking, 4G etc). Many different techniques and parameters are proposed in the literature [6-9] for the selection of appropriate network in heterogeneous networks. These non-standardized, network-specific selection parameter values can be embedded in the beacon itself, thus enabling the stations to always be updated with most recent parameter values. This facilitates the wireless client to always be in a position to decide the best network to which it can connect to, without putting additional overhead on the network.

Moreover, it can be used to advertise location specific services/products because location of APs are known and the physical reach of beacons is limited to the propagation of 802.11 signals. This enables the advertising industry to benefit from it. Consider an example of a trade fair which is an exhibition in which the companies of a specific industry showcase and demonstrate there latest products or services. Such companies can use the beacon frames to advertise there stall locations/products/services to near by potential customers/visitors. This helps the companies to advertise without any additional set up/cost, as well as the visitors/customers as they receive the advertised information on there mobile devices.

Other than the above explained potential usage, A J nicolson et al [2] proposed to use it for reducing the overhead of Dynamic Host Configuration Protocol (DHCP) configuration process while migrating to a new AP. Y Grunenburger et al [3] has used it for piggybacking the signal level in the beacon, thus allowing APs to inform its neighbors on the signal quality with the station. V Mhatre et al [4] uses it in there proposed routing algorithm for mesh networks for embedding information about all active links of a node in the beacon frame. R Chandra et al [5] uses it in there scheme, called Neighborcast, using which the nearby clients can communicate with each other even when they are associated to different APs.

3. BEACON FRAME FORMAT

The following frame format description is valid up to the base IEEE 802.11-2007 protocol [9].

Fig. 1 shows the format of the beacon frame, which is a type of management frame in 802.11. It contains 24 octets of MAC header, 0 to 2312 octets of Frame Body, and 4 octets of Frame Check Sequence (FCS). The Frame Body is a field of variable length and its information contents are specific to individual frame types and subtypes. It consists of two sets of fields, in order: 1) fields that are not Information Elements, followed by 2) fields that are Information Elements. The common general format of all the Information Elements is shown in Fig. 2.

For detailed and correct information about the various fields of the beacon frame, the reader may refer to [9].

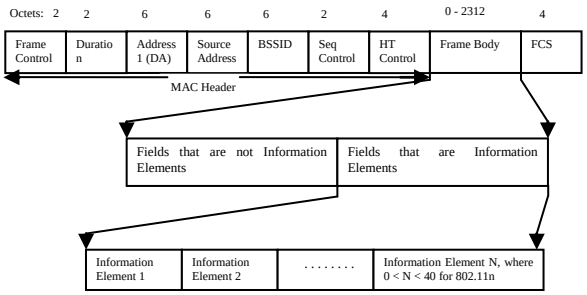

Fig. 1: Beacon Frame Format

4. POTENTIAL FIELDS TO CARRY ADDITIONAL INFORMATION

In this section we explain the various fields of the beacon frame in which the additional non standard information can be embedded. These are proposed by R. Chandra et al [21].

4.1 SSID Field

Utilization of SSID field of the beacon frame for carrying additional information was originally proposed by R Chandra et al [21]. In an Infrastructure BSS, SSID indicates the identity of an ESS (Extended Service Set) and is part of the frame body with ELEMENT ID 0 (zero). Its maximum length can be of 32 octets.

This approach has an advantage of being simple and does not require any kernel modification on client devices. Using this approach, longer messages can be sended at the rate of 23 Kbps [21].

4.2 BSSID Field

BSSID is a six octet field in the MAC header and indicates the MAC address currently in use by the station contained in an AP. It uniquely identifies each BSS. Again, utilization of this BSSID field for carrying additional information was originally proposed by [21].

However, it too has significant limitations. Since its size is fixed to 6 octets only, the information content which can be carried is very limited in size. Moreover, it is always not available to be free. For example, if the Source Address field of MAC header contains a group address, the BSSID also is validated by all the receiving wireless clients.

4.3 "Vendor Specific" Information Element Field

Because of the extensive importance and allowing some flexibility to the vendors, 802.11 standard itself has a provision to carry nonstandard, vendor-specific information in the "vendor specific" Information Element (IE) field of beacon frame. This IE (with ELEMENT ID 221) is provisioned to always be present as a last IE in the frame body of beacon. Using it, up to 253 octets of information can be embedded in each beacon frame.

Though a large amount of information contents can be embedded in this field, it too has a drawback. It requires change in the 802.11 driver at the client device, and of course increase the size of beacon frame.

5. A NOVEL APPROACH FOR INFORMATION EMBEDDING

Other than the above mentioned fields, we found and propose to use the Length field of each IE of the frame body to be a potential candidate for carrying the additional information.

Fig. 2 shows the general format of each IE, where multiple IE's can be the part frame body of the beacon frame.

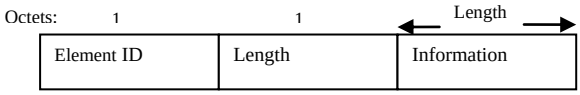

Fig. 2: General Frame Format of Information Element

Each IE contains three fields: 1 octet of ELEMENT ID field, followed by 1 octet of LENGTH field, followed by variable-length element-specific INFORMATION field. Each IE is assigned a unique ELEMENT ID which fits in 1 octet. So 255 different ELEMENT IDs are possible. Out of these, 802.11 has reserved the unspecified IDs. The LENGTH field specifies the length of Element-specific INFORMATION field.

802.11 protocol specifies the minimum and maximum length of each element-specific INFORMATION field. Thus the minimum and maximum value which the one-octet LENGTH field of each ELEMENT ID can take is fixed and known. It is this LENGTH field in which the data gets transmitted without any information . For example, Power Constraint Information Element (with Element ID 32) can have INFORMATION field of one octet only. So, the LENGTH field will always contain the value 1, thus leaving 7 most significant bits to contain value 0 always.

To get the total number of free bits, we compiled the data of all the IE which can be the part of Beacon Frame of 802.11-2007 standard. This compiled information is depicted in Table 1. It shows the 22 IEs which can be the part of Beacon Frame. Order Number indicates the order at which the corresponding IE can be present in the frame body of the beacon frame. Information Element indicates the corresponding name of IE as specified in 802.11. Element ID is the unique ID of corresponding IE. The last column specifies the number of unused most significant bits in Length field.

Table 1 clearly shows that if all the IE are part of the Beacon, we can overload a total of 81 bits (approx 10 octets) of information on it.

The following are the advantages of beacon overloading in the proposed LENGTH Field:

a) To implement this scheme, the change is required in the WLAN driver at the AP and the wireless client station. But this change will not result in changing the MAC layer. It only requires the introduction of a new module which inserts the information bits in the corresponding LENGTH field of the beacon frame. This is because by overloading the information, the meaning and purpose of the fields of the beacon are not changed. Also, once the MAC layer of 802.11 readies the beacon frame and is ready to be delivered to the physical layer through Service Access Points, it can be intercepted by the newly proposed module. The information is then inserted and the frame is forwarded to the Physical Layer.

b) This technique effectively utilizes the channel resources which otherwise are utilized for just transmitting "data" and not any "information".

c) If the information can be embedded in all the LENGTH fields only, there is no extra network resources required for the transmission of information. Of course, the computational resources at the two end point (i.e. AP and wireless client) is required for embedding and extracting the information.

Table 1: Compiled data of number of free bits in LENGTH field of all Information Elements.

S. No.	Order Number	Information Element	Element ID	Unused bits in LENGTH field
1	4	SSID	0	2
2	5	Supported Rates	1	4
3	6	FH-parameter set	2	5
4	7	DS parameter set	3	7
5	8	CF parameter set	4	5
6	9	IBSS parameter set	6	6
7	10	TIM	5	0
8	11	Country	7	0
9	12	FH parameters	8	6
10	13	FH Pattern Table	9	0
11	14	Power Constraint	32	7
12	15	Channel Switch Announcement	37	6
13	16	Quiet	40	5
14	17	IBSS DFS	41	0
15	18	TPC Report	35	6
16	19	ERP Information	42	7
17	20	Extended supported Rates	50	0
18	21	RSN	48	0
19	22	BSS Load	11	5
20	23	EDCA parameter set	12	3
21	24	QoS Capability	46	7
22	Last	Vendor Specific	221	0

6. IMPLEMENTATION

Fig. 3 shows the change required in the WLAN-driver software architecture of AP. The dotted line represents the existing message flow, i.e. the MAC sublayer readies the beacon frame and handover it to PLCP sublayer for transmission. In the modified architecture, instead of handing over the beacon frame to PLCP sub layer, it is handed over to newly added module. This module embeds the vendor/network specific information bits in the LENGTH field using the values of array FB.

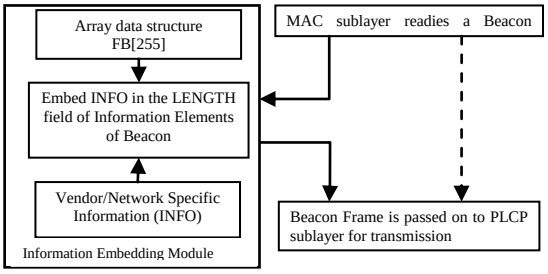

Fig. 3: Software architectural changes required at AP.

The embedding algorithm is shown below. In this algorithm we assumed that the length of information, INFO, to be embedded is fixed and the number of IE in the beacon are sufficient so that all the bits of INFO can be embedded in the corresponding LENGTH fields. Of course the actual algorithm to be implemented will depend on what INFO is to be embedded. For example, If the number of bits in INFO varies with time, we can use the first six free bits in LENGTH fields of first two ELEMENT IDs to represent the number of octets of INFO.

```
IEM_AP_Algo (Beacon beacon, Information INFO)
{
 j=1, i=0;
 while (there are more bits in INFO)
 {
 EID = Element ID of jth Information Element of
 Frame Body of beacon
 N = FB [EID]
 Replace the most significant N bits of LENGTH
 field with the N bits of INFO starting from ith
 position
 i = i + N
 j = j + 1
 }
}
```

Similarly, Fig.-4 shows the change required in the WLAN-driver software architecture of client stations. Again, the dotted line shows the existing message flow and the solid lines shows the modified message flow.

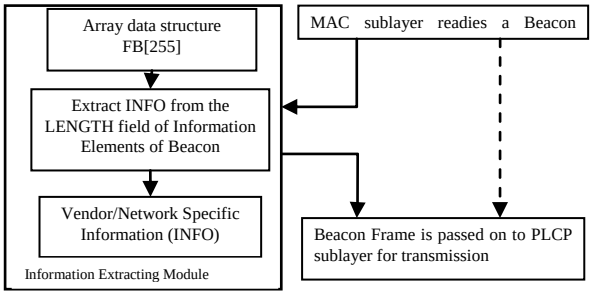

Fig. 4: Software Architectural changes required at the wireless clients.

Following is an algorithm to extract the information at wireless clients.

```
IExM_WC_Algo (Beacon beacon, Information INFO)
{
 j=1, i=0;
 while (there are more bits to be extracted from beacon)
 {
 EID = Element ID of jth Information Element of
 Frame Body of beacon
 N = FB [EID]
 Replace the N bits of INFO starting from ith position
 with most significant N bits of LENGTH field.

 Replace the most significant N bits of LENGTH
 field with 0.
 i = i + N
 j = j + 1
 }
}
```

7. FUTURE WORK

The main future work is to show how this technique can be implemented by suggesting the necessary changes required in the WLAN driver at the AP and the mobile terminal. Also, with the launch of the latest IEEE 802.11-2012 base standard, it is required to study that how many more free bits are there in the LENGTH field.

8. CONCLUSION

Considering the IEEE 802.11-2007 protocol, in this paper we have shown that in a beacon frame there are few fields which can be utilized to carry additional non standard information without breaching the standard. Other than the fields proposed by R. Chandra et al [21], we show that the Length field of the IEs is also the potential candidate for the same. Using it, about 10 octets of additional non standard information can be broadcasted without consuming any extra channel/network resources. Of course, how to use these fields and what information is to be embedded depends upon the application requiring it.

9. REFERENCES

[1] Gupta V., Rohil M. K., Mobile Data Offloading: benefits, issues, and technological solutions. Advances in Computer Science, Engineering & Applications, Springer Berlin / Heidelberg, Volume: 167, pp 73-80, 2012.

[2] Nicholson A.J., Wolchok S., Noble B.D. Juggler: Virtual Networks for Fun and Profit. IEEE Transactions on Mobile Computing, vol.9, no.1, pp.31-43, Jan. 2010

[3] Grunenberger Y., Rousseau F. Virtual Access Points for Transparent Mobility in Wireless LANs. In proceedings of IEEE Wireless Communications and Networking Conference (WCNC) (Sydney, Australia, April 18 - 21, 2010)

[4] Mhatre V., Lundgren H., Baccelli F., and Diot C. Joint MAC-aware routing and load balancing in mesh networks. In Proceedings of the 2007 ACM CoNEXT conference (CoNEXT '07). ACM, New York, NY, USA, , Article 19 , 12 pages.

[5] Chandra R., Padhye J., Ravindranath L. Wi-Fi Neighborcast: Enabling Communication Among Nearby Clients. Proceedings of the 9th workshop on Mobile computing systems and applications. (Napa Valley, California, February 25-26, 2008).

[6] Chen W., Liu J. C., Huang H. An adaptive scheme for vertical handoff in wireless overlay networks. In proceedings of tenth international conference on Parallel and Distributed Systems, ICPADS 2004. (Newport Beach, California, July 7-9, 2004)

[7] Hasswa A., Nasser N., Hassanein H. Tramcar: A Context-Aware Cross-Layer Architecture for Next Generation Heterogeneous Wireless Networks. In proceedings of IEEE international conference on communications. (Istanbul, Turkey, June 11 - 15, 2006)

[8] Tawil R., Pujolle G., Salaza O. A Vertical Handoff Decision Scheme in Heterogeneous Wireless Systems. In proceedings of Vehicular Technology Conference. (Marina Bay, Singapore, May 11 - 14, 2008)

[9] IEEE standard 802.11. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications, 2007

[10] IEEE standard 802.11k. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 1: Radio resource management of wireless LANs, 2008.

[11] IEEE standard 802.11r. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 2: Fast Basic Service Set (BSS) transition, 2008.

[12] IEEE standard 802.11y. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 3: 3650 - 3700 MHz operation in USA, 2008.

[13] IEEE standard 802.11w. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 4: Protected Management Frames, 2009.

[14] IEEE standard 802.11n. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 5: Enhancements for Higher Throughput, 2009.

[15] IEEE standard 802.11p. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 6: wireless access in vehicular environments, 2010.

[16] IEEE standard 802.11z. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 7: Extensions to Direct-link setup (DLS), 2010.

[17] IEEE standard 802.11v. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications - amendment 8: IEEE 802.11 wireless network management, 2011.

[18] IEEE standard 802.11u , Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications – amendment 9: interworking with external networks, 2011

[19] IEEE standard 802.11s, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications – amendment 10: Mesh Networking, 2011

[20] Zhu f., McNair J. Optimizations for vertical handoff decision algorithms. In proceedings of IEEE wireless communications and networking conference (Atlanta, USA, March 21-25, 2004).Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.

[21] Chandra R., Padhye J., Ravindranath L., Wolman A. Beacon-Stuffing: Wi-Fi without Associations. In Proceedings of the Eighth IEEE workshop Mobile Computing Systems and Applications (Tucson, Arizona, February 26-27, 2007).