Bit-Stuffing in 802.11 Beacon Frame: Embedding Non-Standard Custom Information

Vishal Gupta
Birla Institute of Technology and Science, Pilani
Pilani, India

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

ABSTRACT
In an infrastructure Basic Service Set (BSS) beacon frames are transmitted periodically by the Access Point (AP) and announce the presence of a wireless network. It mainly consists of network specific information and thus one of its main purposes is the "advertisement" of this information. Based on this information mobile devices can take many decisions, for example, whether to attempt association with the network or not. To facilitate the communication between devices developed by different vendors, IEEE 802.11 standardizes the arrangement of this information in beacon frames. Often it is required to embed non-standard vendor/network specific additional information in the beacon frame. In this paper we show that without disturbing the arrangement of information as per the standard, how the IEEE 802.11-2012 compatible beacon frames can be overloaded with additional non-standard information. Moreover, the 802.11 standard limits the maximum size of the beacon frame. In this perspective we also show that how to send large amount of information in multiple successive beacon frames using the already implemented concept of fragmentation and sequence numbers. The proposed technique is flexible in terms of fields used for embedding the information and maximizes the number of additional non-standard information octets per beacon. The results of its implementation in ns-3 simulator are also shown.

General Terms
Beacon Stuffing, 802.11 beacons, Wi-Fi ads.

Keywords
IEEE 802.11-2012, Beacon, Information Element, Beacon Stuffing.

1. INTRODUCTION
Over the years 802.11 technologies has emerged as one of the dominant technology for Wireless Local Area Network (WLAN). It is the basis for wireless network products using the Wi-Fi brand. Because of its capability of providing data at sufficiently high data rates and its feature of operating at unlicensed spectrum it has become so popular that most of the wireless devices today are 802.11 compatible. Also because of its complementary characteristics to cellular networks, it has emerged as one of the most prominent choice for Mobile Data Offloading [2, 24].

Beacon frame is a type of management frame as per 802.11 standards and is broadcasted periodically by the Access Point. The period between the two beacon frames is configurable and varies from network to network. If a mobile device needs to communicate using the 802.11 network, it first listens to the beacon frame. Using the information embedded in it, the device decides whether to connect to it or not. If yes, it attempts Association with the corresponding Access Point (AP).

Mostly beacon frame carries the information related to the network with which the corresponding associated AP broadcasted it. The syntax, semantics and arrangement of this information in the beacon is standardized by 802.11 standard. This is to facilitate the communication between any two 802.11 compatible devices, especially when they are manufactured by different vendors.

The mobile devices which had activated (or turned ON) there respective 802.11 network interfaces inherently receives all the beacon frames of the corresponding networks in the vicinity. So, other than serving the purpose as specified in the standard, the beacon frame can be looked upon from a different perspective: a carrier which is advertising the information to the mobile devices in the vicinity. Often this perspective of the beacon frame is exploited in numerous ways. In section III we discuss few of them. Here the meaning of the word advertisement is not restricted to only commercial products advertising, rather it means inherent broadcast of any information.

This advertising perspective of the beacon frame often requires embedding additional non-standard information in it without disturbing/changing the arrangement of information as per the standard. R. Chandra et al [1] had proposed to use SSID, BSSID, and Vendor Specific fields of 802.11 beacon for carrying such information. In this paper, other than the BSSID and Vendor Specific fields (Section II discusses upon the short comings of SSID field for stuffing information), additionally we propose to use Length fields of all Information Elements. More specifically, in addition to BSSID and Vendor Specific fields, we show that considering IEEE 802.11-2007 standard and all its ten amendments (and thus IEEE 802.11 - 2012 standard), up to 24 octets of data, and not information, always gets transmitted in Information Element fields of every beacon frame. We propose to exploit these Information Elements to embed any additional information in them. Also, 802.11 standard specifies the maximum size of the beacon frame. Using it the amount of additional information to be embedded in the three proposed fields is maximized. It is also shown that how to do fragmentation of the large chunk of data such that it can be embedded in multiple successive beacon frames.

The scope of our work is limited to the following:

a) The ideas and results presented are valid up to the standard IEEE 802.11-2012 published in March 2012 [22]. This standard incorporates Amendments 1 to 10 [11 - 20] of base IEEE 802.11-2007 standard [10], published since 2008 to 2011.

b) Many operation modes can be supported by WLAN devices. These are infrastructure, ad hoc, virtual access point, wireless distribution system, mesh, virtual interface and monitor. Everything presented in this paper is related to infrastructure mode only. Of course, further research can be done for other modes of operation also.

The rest of the paper is organized as follows. Section 2 discusses the work of R Chandra et al [1] and its short comings. Section 3 discusses the applications of embedding additional information in the beacon frames. Section 4 describes beacon frame format. As a novel contribution, Section 5 shows the unused bits available in the Length field of Information Elements. Section 6 explains the proposed technique. Section 7 discusses upon the simulation results, and finally showing future extensions of the scheme the paper concludes.

2. DISCUSSION ON RELATED WORK

For a wireless device/client to communicate with the AP, it should first attempt Association. Without Association established, the communication cannot happen [10, 22]. Ranveer Chandra et al [1] had proposed a low bandwidth communication protocol using which the wireless clients can receive information even if they are not associated with the AP. This protocol is based on two key observations: wireless clients always receive the beacon frames from APs even if there is no association established, and beacon frame can be overloaded with more data. Following are the fields proposed to stuff additional data/information [1]:

2.1 Subscription Service Identifier (SSID)

In an Infrastructure BSS, SSID indicates the identity of an Extended Service Set (ESS). In other words it is a network name because essentially it is a name that identifies a wireless network and all wireless devices on a WLAN must employ the same SSID in order to communicate with each other. It can be up to 32 alphanumeric character unique identifier [24]. It is the part of the frame body of the beacon frame with ELEMENT ID 0 (zero).

2.2 Basic Service Set Identifier (BSSID)

It is always present as a part of Medium Access Control (MAC) header in the beacon frame and is a 6-octet field. It uniquely identifies each BSS. More specifically, it indicates the MAC address currently in use by the station contained in an AP.

2.3 Vendor Specific Information Element

To allow flexibility to the vendors for implementing the optional functions and proprietary features, 802.11 standard has a provision to carry vendor-specific non-standard information in the beacon frame. As shown in figure-1 there are many Information Elements which can be the part of frame body of the beacon frame. Vendor Specific Information Element (with Element ID 221) will always be the last Information Element and can carry information contents up to 252 octets.

Though technique proposed by R Chandra et al [1] successfully overloads the three fields of the beacon frame with additional data, it has certain limitations as listed below:

1) Approach of embedding information in SSID field has an advantage of being simple and it does not require any kernel modification on client devices. Despite its advantages, this approach has a significant limitation. According to 802.11, SSID Information Element indicates the identity of an ESS. Many client devices (for example smart phones, iPhones, laptops etc) display each unique SSID in the received beacons of all the 802.11 networks with in the range to facilitate the end user in network selection. If one AP is sending fragments of a large message chunk embedded in SSID field of subsequent beacons and the AP beacon interval is assumed to be 10 milliseconds [1], each client device in the region will display 100 "bogus" SSIDs per second. And if multiple APs within the range are using SSID field for stuffing bits, the situation will become even worse for the client device. In fact, the legitimate SSIDs will virtually be lost and it will be extremely difficult for the client to decide on the network to which to attempt Association to. Because of these reasons, in this paper SSID field will not be used for embedding additional information. Of course, we can use delimiters to partition the used SSID's with that of unused ones, this aspect is left for future work.

2) The limitation with BSSID is that it is not always free, for e.g., if the Source Address field of MAC header contains a group address, all the receiving stations (or wireless clients) also validate the BSSID. If it is free also then the information content it can carry is limited to 6 octets only. Moreover, stuffing data in BSSID and Vendor Specific fields requires significant changes in the corresponding WLAN drivers at the AP as well as the mobile device.

3) The fragmentation technique proposed uses explicit sequence numbers. But those are redundant because beacon frame already has 12-bit sequence number field in the sequence control field structure of MAC header, and it can be used to the same effect. Beacons not received in order will automatically generate error in the driver code.

4) SSID concatenation, BSSID concatenation and Vendor Specific Elements could send only 32, 6, 252 octets respectively. The maximum size of beacon frame body is 2320 octets [22], and a lot more data could be embedded to increase the transmission rate.

5) The technique uses only one Vendor Specific IE to carry the data. But, according to IEEE 802.11 standards, multiple Vendor Specific elements can be added as long as the maximum size of the beacon is not exceeded.

6) Though three fields have been listed; they are used independently of each other. Combining multiple fields/approaches will lead to a greater transmission rate.

3. APPLICATIONS OF OVERLOADING INFORMATION IN BEACON FRAME

The principle benefit of embedding addition information in the beacon frames is that they can be read and processed by the wireless client without associating with the corresponding AP. Also, the beacon frames can be received only within a limited physical range in which the wireless network is available, thus inherently facilitating Location Based Services (LBS). This makes several applications, which would otherwise require complex algorithms and techniques, to be easily implemented. Some of the major applications are as follows:

3.1 Network Selection in 3G-WLAN Interworking Environments

3G WLAN internetworking is an ongoing standardization work item in third Generation Partnership Project (3GPP). The aim is to combine the ubiquitous data coverage of 3G and the high-speed data service offered by WLAN networks into a seamless wireless network. For it, many 3G-WLAN interworking models are been proposed by researchers in the

literature. X. Yan et al [25] and M. Kassar et al [26] present an elaborative survey of these models. The proposed models mainly differ with respect to the parameters (such as, pricing, number of active users, user preferences etc.) considered for deciding the network to connect to. To make these models practically useful requires making the values of these parameters available to the mobile device. Another useful constraint towards making a seamless vertical handover is to make these values available without enforcing the mobile device to connect to the network. Now, with this constraint, since beacon frame is the only communication frame received by the mobile device, stuffing additional bits in it is a viable (and in fact essential unless another special frame is designed for the purpose) option.

3.2 Location specific advertisements/ Services and coupons:

Location specific advertisements are beneficial both to the marketers and the target audience. Location awareness helps in building applications to broadcast useful information like that of nearest ATMs, Gas stations etc. Now since the location of AP is known and the coverage area of the AP is limited, inherently the approximate location of the mobile station from the AP is also known. Moreover, the exact location of the AP may also be transmitted as embedded data, saving the need of GPS and conserving battery life of devices while improving the accuracy. This aspect serves as a useful means for many location aware applications. So, in this case, the additional information overloaded in the beacon would be these advertisements we wish to serve. There are multiple advantages to approach. The user doesn't need to have an active Internet connection. The problem to locate the user within the specific location has been solved without using Global Positioning Service (GPS), which is either battery drainer or not so common. The wireless client always listens passively to the presence of beacon frames, and thus the advertisements would be delivered to them without any extra effort on their part.

This approach similarly can be used to broadcast coupons about offers and discounts, announcements by shops, etc.

Moreover, the concept of embedding additional information in the beacon frame is been used by a number of applications. A J Nicolson et al [3] have used it to increase efficiency of the mobile station with reduced overhead of Dynamic Host Configuration Protocol (DHCP) configuration process when mobile device is migrating to a new AP. V Mhatre et al [5] used it for embedding information about all the active links of a node in there proposed routing algorithm for mesh networks. Y Grunenburger et al [4] used it for allowing AP's to inform its neighbors about the signal quality. This signal quality was piggybacked on the beacon frames. R Chandra et al [6] used it in there scheme, called Neighborcast, which allows the nearby mobile stations to communicate with each other even when they are associated to different APs.

4. BEACON FRAME FORMAT

The IEEE 802.11 beacon frame format is shown in Figure- 1. The 28 octets long frame header (or MAC header) consists of Frame Control, Duration, Address 1, Source Address, BSSID, Sequence Control and HT Control fields. The header is followed by the variable length Frame Body, which can be up to 2320 octets long. Frame Check Sequence (FCS) is a 4-byte long field used to perform cyclic redundancy check for validating the received frames. The frame body consists of a series of fields that are classified as fields that are not Information Elements followed by fields that are Information Elements. Information Elements appear in a fixed relative order and are identified by respective unique Element ID. The general format of all the Information Elements is shown in Figure 2.

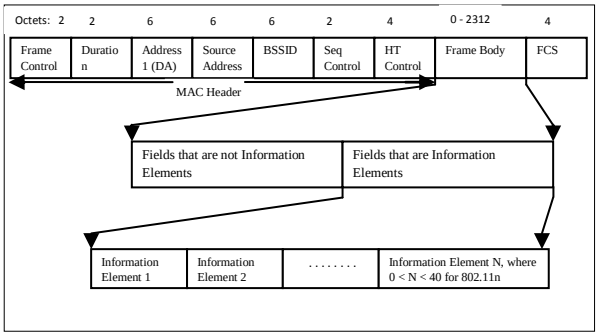

Fig 1: Beacon Frame format of 802.11

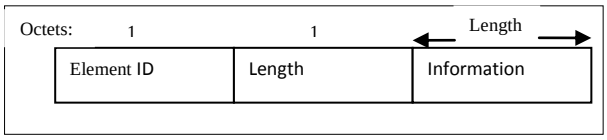

Fig 2: General format of Information Element

Each Information Element has following three fields:

1) 1-octet long Element ID (EID) field to uniquely identify the Information Element. Hence, 256 unique Information Elements are possible. As per 802.11-2012, up to 53 EID's can be the part of beacon frame.

2) 1-octet long LENGTH field.

3) LENGTH-octet long INFORMATION (Data) field. Thus the maximum length of INFORMATION field can be 255 octets.

5. EMBEDDING INFORMATION IN LENGTH FIELD OF INFORMATION ELEMENTS

Other than BSSID and Vendor Specific fields, in this section we show the bits which get transmitted in each beacon frame and on which additional information contents can be overloaded.

Figure-2 shows the general format of each Information Element. ELEMENT IDs are numbered from 0 to 255. Out of these, the unspecified ELEMENT IDs are reserved by IEEE. Corresponding to each ELEMENT ID the LENGTH field specifies the exact length of the INFORMATION field.

Though the INFORMATION field is a variable length field, its minimum and maximum length is been fixed by 802.11 standard. In other words, the minimum and maximum value which can be stored in the LENGTH field of each ELEMENT ID is known and fixed. Since one octet is been assigned to LENGTH field and there are many INFORMATION fields whose maximum length will always be less than or equal to 255, it is these LENGTH fields of Information Elements which makes it suitable for carrying additional information. For example, BSS Average Access Delay Information Element (with Element ID 63) can have maximum length of INFORMATION field to be 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 Information Elements, which can be the part of beacon

frame up to 802.11-2012 standard. This standard includes all the ten amendments to IEEE 802.11-2007 standard. Since all the WLAN's does not necessarily implement the functionality of all the ten amendments, we also compiled the information about free bits for each individual amendment. This is shown in Table-II of Appendix-1. Figure-3 shows the graph depicting total number of free bits available with each successive amendment to IEEE 802.11-2007.

Table II clearly shows that if all the Information Elements are part of the beacon, we can overload 191 bits of additional information in the LENGTH field.

5.1 Advantages of Embedding the Information in the LENGTH field

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

a) To implement the information embedding in the LENGTH field, the WLAN drivers are required to be modified at the AP and the mobile device. Though it appears to be a limitation, it is not because using BSSID and Vendor specific fields also requires changes in the drivers.

b) This technique is scalable. This is because when the functionality of an existing WLAN is to modified/extended to include any new amendment, the change required in the driver is minimal; in fact only array data structure, FREE_BITS (explained in section VI), needs to be changed. The rest of the embedding function will remain as it is.

c) The utilization of channel resources is optimized which otherwise was used for only transmitting "data" and not any "information".

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

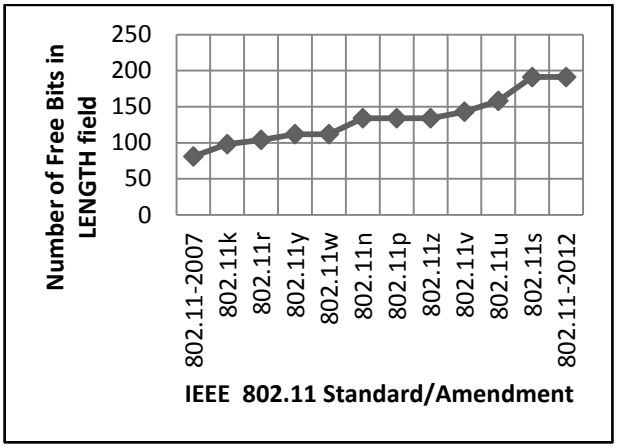

Fig 3: Free Bits with each successive amendment to IEEE 802.11-2007

6. PROPOSED TECHNIQUE FOR STUFFING INFORMATION IN THE BEACON

6.1 Fields for embedding information

Depending upon the length of the information to be embedded, the proposed technique uses the following three fields for embedding additional information, preferably in order. It overcomes the limitations of earlier approach [1]:

a) BSSID field: If it is free then it is preferred over Length and Vendor Specific Information Element. This is because, whether free or not, BSSID will always be present as a MAC header and thus always gets transmitted. If INFOLEN is the length of the information to be embedded, the first six octets of INFOLEN are stuffed in it.

b) LENGTH field of Information Elements as explained in Section - V above. It is preferred over the Vendor Specific field because it also gets transmitted always, thus embedding information does not increase the size of the beacon. The number of free octets (FLEN) in all the Length fields is calculated first because the number of Information Elements which can be the part of beacon is not fixed and depends upon the functionality implemented at the AP. The FLEN octets of information starting from the seventh octet of INFOLEN are stuffed into it.

Also, for embedding information in the LENGTH fields of the Information Elements, an array data structure is used. It is defined as integer FREE_BITS[255], where FREE_BITS [i] is the maximum number of available bits in the LENGTH field corresponding to ELEMENT ID [i], $0 <= i <= 255$. Since the protocol (and all its successive amendments) has fixed the maximum length of INFORMATION field corresponding to each ELEMENT ID, the values in this array are fixed up to a particular amendment. Only when the functionality of a new amendment is to be implemented, this array values need to be changed.

c) Vendor Specific Information Element: A beacon can have multiple Vendor Specific Information Elements as long as the size of the beacon is less than the maximum size allowed (i.e. 2320 octets [22]).This is at the last priority and the next (up to) [2320-(INFOLEN - (FLEN+6))] octets of INFOLEN, starting from the (FLEN+7)th octet of INFOLEN are stuffed into it.

6.2 Fragmentation

If the size of INFOLEN is large such that the complete information cannot be stuffed in a single beacon, the information can be fragmented such that multiple successive beacons can be stuffed with the fragmented parts. To indicate fragmentation, only 1 bit is sufficient. If the bit reads 0, that would imply that it is the last fragment or trivially that it is the only fragment. If the bit reads 1, it would imply that more fragments would follow.

Since the Length field of SSID Information Element has most significant two bits free and is always present in the frame body of the beacon, the bit to indicate fragmentation is added to it. The mobile device reassembles the information by using this fragmentation bit and the 12-bit sequence number of the sequence control field structure of MAC header.

6.3 Control Information

To signify to the client device about the fields (out the three proposed) in which the additional information is stuffed, control information is required to be passed. For it, the Length field of another Information Element (called Supported Rates) is utilized. It is also always the part of frame body of the beacon frame and has four unused bits in the Length field. These are used to carry control information as specified in Table 1.

Table 1: Control bits and the associated meaning

Control Bits	Associated Meaning
000	No information is carried
001	Only BSSID has additional information
010	Only Length fields of IE's has additional information
011	BSSID and length fields together has additional information
100	Only vendor specific elements has additional information
101	BSSID and vendor specific elements together has additional information
110	Length fields and vendor specific elements together has additional information
111	All three fields has additional information

6.4 Data Integrity Check

Each beacon frame has 32-bit Frame Check Sequence (FCS) field containing a 32-bit CRC. It is calculated over all the fields of the MAC header and the Frame body field. This covers the embedded information as well.

At the receiving end, depending upon the control information, the embedded information from the corresponding fields is extracted and stored in the buffer. While extracting the information, using FREE_BITS array data structure the most significant bits of the Length fields carrying custom information is made 0, i.e. bring it into the format as required by other driver functions. Finally, if the beacon has the last fragment of custom information, the contents of the buffer are readied to be delivered to the upper layers.

7. SIMULATION AND RESULTS

The proposed scheme for stuffing additional bits in the beacon frame was successfully implemented in network simulator 3 (ns-3). For simulation a BSS having one AP and two mobile stations was considered. By default in ns-3 only two Information Elements (i.e. SSID and Supported Rates) are part of the beacon frame body. So, following three things were selected randomly for simulation:

a) From 802.11-2012 standard, number of Information Elements to be added to the frame body of the beacon.

b) Information in terms of number of characters (with each character taking one octet) to be embedded.

c) Out of three fields proposed in section VI, which fields are to be utilized for stuffing the characters. This is for showing the flexibility of the technique.

Using the above three aspects (and fragmentation), the information was successfully stuffed in the beacon transmitted by the AP and was extracted successfully at both the mobile stations.

Moreover, the amount of custom information that can be embedded in the beacon frame has also been maximized as shown in figure 4. The graph shows the amount of information that can be added versus each additional IE. Adding another IE after the one with EID 64, would exceed the size of the beacon and hence, is not listed on the graph. The amount of information is represented on a logarithmic scale.

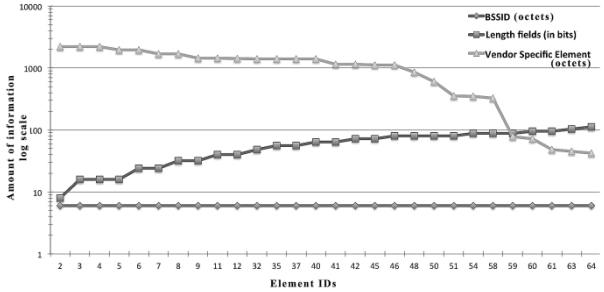

Fig 4: Amount of information that can be added versus each additional IE.

8. FUTURE WORK

The Information Elements which are not the part of beacon frame also has free bits in LENGTH field. We would like to extend our work to study these for possible usage in other frame types.

9. CONCLUSION

Over the years Wi-Fi network has emerged as one of the most promising technology for WLAN. Also, the complementary characteristics of 802.11 network to cellular network has a major contribution in the wide spread reach and usage of Wi-Fi networks. To announce the presence of Wi-Fi network in the vicinity the corresponding AP periodically broadcast the beacon frame. This frame mainly consists of the network specific parameters. This "broadcasting", "location-specific", and "advertising" perspective of the beacon frame has opened the possibility of many other application areas, for example, assisting network selection in the heterogeneous wireless networks, location specific advertisements, etc. In this paper the work of R Chandra et al [1] is extended for stuffing additional information in the IEEE 802.11-2012 compatible beacon frame. More specifically, as earlier advocated, we had shown the hazardous effects of using SSID field for this purpose. Rather, as a novel contribution, the Length field of the Information Elements is been shown to have unused bits, and thus advocated to be used for stuffing additional information. The technique proposed uses this Length field along with the earlier proposed BSSID and Vendor Specific fields. The proposed technique also maximizes the additional non-standard information contents in the beacon frame, and uses fragmentation for embedding large information using already available sequence numbers field in multiple successive beacon frames. Finally, the scheme is successfully implemented in ns-3 simulator.

10. REFERENCES

[1] 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)

[2] Gupta V., Rohil M. K. Mobile Data Offloading: benefits, issues, and technological solutions. Advances in Intelligent and Soft Computing, Springer Berlin / Heidelberg 2012, vol 167 pp 73 - 80.

[3] 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

[4] 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)

[5] 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.

[6] 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).

[7] 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)

[8] 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)

[9] 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)

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

[11] 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.

[12] 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.

[13] 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.

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

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

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

[17] 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.

[18] 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.

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

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

[21] 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)

[22] IEEE standard 802.11. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer specifications, 2012

[23] Vipin M., Srikanth S. Analysis of Open Source Drivers for IEEE 802.11 WLANs. In proceedings IEEE conference of ICWCSC 2010.

[24] Gupta V., Rohil M. K.. Enhancing Wi-Fi with IEEE 802.11u for Mobile Data Offloading. International Journal of Mobile Network Communications & Telematics. vol 2, no. 4, August 2012.

[25] X. Yan, Y. A. Sekercioglu, S. Narayanan. A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks, Computer Networks, Volume 54, Issue 11, August 2010, pp 1848-1863.

[26] M. Kassar, B. Kervella, G. Pujolle. An overview of vertical handover decision strategies in heterogeneous wireless networks, Computer Communications, Volume 31, Issue 10, June 2008, Pages 2607-2620.

APPENDIX I

Table 2 shows the following columns:

1. **Order number**: It is a relative order in which the elements are present in Beacon.

2. **Element ID**: It uniquely identifies each Information Element. The base standard 802.11-2007 had only 21 defined information elements and more have been added with the amendments to it.

3. **Information Element**: Name of Information Element as per 802.11.

4. **Max Length Field**: The Maximum length of LENGTH field as specified in 802.11.

5. **Number of Free Bits in LENGTH field**: The number of free bits in each Information Element and up to 802.11-2012. The total is 191 bits.

Table 2: Number of Free Bits present in each IE

S.no	Order Number	Information Element	Element ID	Max Length Field	Number of free bits in Length Field
IEEE 802.11-2007					
1	4	Service Set Identifier (SSID)	0	32	2
2	5	Supported rates	1	8	4
3	6	Frequency-Hopping (FH)	2	5	5
4	7	DS Parameter Set	3	1	7
5	8	CF Parameter Set	4	6	5
6	9	IBSS Parameter Set	6	2	6
7	10	Traffic indication map (TIM)	5	254	0
8	11	Country	7	254	0
9	12	FH Parameters	8	2	6
10	13	FH Pattern Table	9	254	0
11	14	Power Constraint	32	1	7
12	15	Channel Switch Announcement	37	3	6
13	16	Quiet	40	6	5
14	17	IBSS DFS	41	253	0
15	18	TPC Report	35	2	6
16	19	ERP Information	42	1	7
17	20	Extended Supported Rates	50	255	0
18	21	RSN	48	254	0
19	22	BSS Load	11	5	5
20	23	EDCA Parameter Set	12	18	3
21	24	QoS Capability	46	1	7
802.11k					
23	25	AP Channel Report	51	255	0
24	26	BSS Average Access Delay	63	1	7
25	27	Antenna Information	64	1	7
26	28	BSS Available Admission	67	24	3
27	29	BSS AC Access Delay	68	4	5
28	30	Measurement Pilot Transmission	66	255	0
29	31	Multiple BSSID	71	255	0
30	32	RRM Enabled Capabilities	70	5	5
802.11r					
31	33	Mobility Domain	54	3	6
802.11y					
32	34	DSE Registered Location	58	20	3
33	35	Extentended Channel Switch	60	4	5
34	36	Supported Regulatory Classes	59	253	0
		802.11n			
35	37	HT Capabilities	45	26	3
36	38	HT Operation	61	22	3
37	39	BSS Coexistence	72	1	7
38	40	Overlapping BSS Scan Parameters	74	14	4
39	41	Extended Capabilities	127	6	5
802.11v					
40	42	FMS Descriptor	86	255	0
41	43	QoS Traffic Capability	89	3	6
42	44	Time Advertisement	69	16	3
802.11u					
43	45	Interworking	107	9	4
44	46	Advertisement Protocol	108	variable	0
45	47	Roaming Consortium	109	1	7
46	48	Emergency Alert Identifier	112	8	4
802.11s					
47	49	Mesh ID	114	32	2
48	50	Mesh Configuration	113	7	5
49	51	Mesh Awake Window	119	2	6
50	52	Beacon Timing	120	253	0
51	53	MCCAOP Advertisement	174	6	5
52	54	MCCAOP Advertisement	123	255	0
53	55	Mesh Channel Switch Parameters	118	6	5