IEEE P802.11
Wireless Access Method and Physical Layer Specifications

Title: Proposal to include a "Prefered IV" list in a Beacon frame.

Author:
Wim Diepstraten
AT&T WCND
Nieuwegein The Netherlands
Tel: (31)-3402-97482
Fax: (31)-3402-97555
Email: Wim.Diepstraten@utrecht.attgis.com

Abstract:
This document proposes to add a "Prefered IV List" field in the Beacon, which can suggest to stations that a potential better performance can be expected when stations use the indicated current IV values.

Introduction:
The security level of the WEP defined as part of the 802.11 draft standard does depend on the frequency with which the IV is being changed.
The use of this scheme can range from implementations with a different IV per frame to implementations that can use a BSS wide "prefered IV", where the AP can determine the frequency with which the IV is changed.
The intend is to allow different levels of implementation of the WEP, from a SW, hybrid SW/HW or HW implementation of the cryptographic algorithm.
The Hybrid solutions are of specific interrest, because this allows implementations where a key string can be generated off line in SW, after which it can be reused several times, requiring only an EXOR function to encrypt or recover the clear text, which can simply be done on-the-fly.
This allows stations to make a tradeoff between extra power consumption and extra latency associated with every change of the IV, and the security level of the used WEP mechanism.

Effect of IV update strategies.

As discussed the performance of certain WEP implementations can largely be affected by the frequency with which a given IV is changed, which directly influences the reuseability of a preprocessed key string.
Low cost stations may shoose to do the pseudo random key string generation in SW, by preprocessing a key string sequence, such that the only "real time" operation needed is an EXOR operation. If stations are forced to process a new key string with every received

frame when the IV changes per frame), then that can highly affect its power consumption and delay (latency) of a frame.
So even when an AP would be capable of on-the-fly encryption so that it could use a new IV per frame (for optimal security), then that would still largely affect user throughput, depending on a stations implementation.

So the user throughput (and power consumption) may benefit a lot when an AP can provide facilities such that a station can reuse a given IV for a number of frames.
This functionality can be achieved when the AP can somehow indicate to a station which IV is prefered for the frame transmissions, and to possibly indicate the next IV.

Use Beacon to distribute a "Prefered IV"

It is assumed that time resolution of Beacon intervals allows for a sufficient IV update frequency if IV reuse at an acceptable security level is the goal.
In that case the AP can distribute a "Prefered IV list" in the Beacon frame, allowing for an IV update at every integer multiple of a Beacon interval, as determined by the AP.

Please note that this does not preclude stations to use a different IV, or that stations update their IV at every frame. They can still tradeoff the gain in security level against a possible increase in power consumption and latency, depending on their implementations.

The "Prefered IV list" should include a "Current IV" and possibly a "Next IV" entry, in which:

- The "Current IV" indicates the IV used by the AP to transmit its frames during the next Beacon interval. Stations who have traffic buffered at the AP could preprocess their key string.
- The "Next IV" indicates what the IV will be in the next Beacon interval, or after the next IV update. This would allow stations to anticipate what IV can best be used for their transmissions, such that they can use the same IV for transmission and reception in the next Beacon interval.

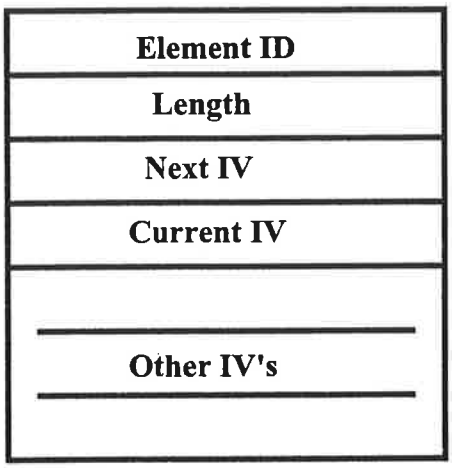
In addition the list could contain a list of "Active IVs in AP", which if present could indicate to a station that the AP can also provide higher performance if one of these IV's are used for transmission by the station.
A special IV of "All ones" could indicate that an AP has no preference, so that any IV use by a station would yield the same performance impact.

Sinse the length of the list is variable or even optional, the "Prefered IV List" should be an element.

Prefered IV List element proposal

The following element format is proposed:

Next IV	Will be the IV after the next update period.
Current IV	Used by AP for traffic during next IV update period.
Other IV's	An all ones entry illustrates no preference.



1 Octet
1 Octet
3 Octets
3 Octets
(0 to n) * 3 Octets

Additional fields are probably needed in the Capability Information field or an other field in (re)Association frames to yield sufficient control.
AP's could indicate whether they support an IV coordination approach.
Stations may want to indicate whether they want to use the IV coordination provisions. If they prefer to use a different IV per frame, and accept possible consequences, then they would likely not want that their "Down frames" are transmitted using the IV coordination approach.