CHAPTER 5

RESULTS AND DISCUSSIONS

PATTERN OF KEYS ANDREAMS GENERATED USING VARIOUS TRANSMISSION RATE

The proposed architecture model for enhancement to TKIP Key mixing using Transmission Rate of PLCP is based on standard 802.11b infrastructure mode. Infrastructure mode supports two Access Points which connect wired network infrastructure and a set of wireless end stations and also act as bridge between the wireless media and wired media. The AP handles station authentication and association to the wireless network.

The current PHY supports any one of the Rate Adaptation Algorithm specified in the chapter 2.11 which supplies signal rate information to PHY layer. The mobile stations may be moving or static, but mobile devices should be under the coverage area of fixed AP.

The proposed architecture for WLAN security mechanism generates a stream of keys at each varying signal rate (such as SIGNAL RATES 1, 2.5, 6, 9, 11, 12, 18, 24) as shown in the following Figures 5-1 to 5-9.
5.1 Pattern of key streams:

Figure 5-1  Key stream patterns generated when signal rate is 1

Figure 5-2  Key stream patterns generated when signal rate is 2
Figure 5-3 Key stream patterns generated when signal rate is 5

Figure 5-4 Key stream patterns generated when signal rate is 6
Figure 5-5  Key stream patterns generated when signal rate is 9

Figure 5-6  Key stream patterns generated when signal rate is 11
Figure 5-7  Key stream patterns generated when signal rate is 12

Figure 5-8  Key stream patterns generated when signal rate is 18
5.2 ANALYSIS ON KEY STREAMS

The following Table 5-1 shows the key stream values generated during the time of encryption for different signal rates, when the order of key sequence is 1, 26, 51, 81 respectively. When base WEP key is changed during every transmission, new IV/base WEP key pairs are used, and unique packet keys will be generated. The mechanism breaks one to one relation between TKIP per-packet encryption keys and WEP IV.
When analyzing the key values generated, it clearly shows that key values are unique, not repeated, dynamic and un-predictable. Encryption is performed by XORing the generated keystream with the plaintext. Decryption consists of generating the identical keystream based on the IV and signal value (secret key) and XORing it with the ciphertext.

Here various keystream patterns are generated for each different transmission rate value. So, keystream reuse can be avoided. The signal value (secret key) remains unknown and maintains the security of the keystream. The use of a dynamic key streams definitely prevent keystream reuse attacks. So the entire system will maintain data confidentiality and integrity.

The Encryption Key Stream is not repeated at any time which means, the cipher text generated by this key stream is never breakable which leads to maintain one of the security measures, confidentiality in WLAN. Passive attacks such as eavesdropping and Traffic Analysis can be avoided. Every station uses the dynamic keys, amount of traffic may
not be available to an eavesdropper for analytic attacks. Active attacks such as replay, message modifications, denial of service can also be avoided.

This new key mixing mechanism highlights the following advantages, firstly, due to varying signal rate and MAC addresses difference, every station will generate different set of WEP per packet encryption keys which eliminates key reuse problem in WEP, secondly, the mechanism breaks any one to one relation between TKIP per-packet encryption keys and WEP IV, lastly, the mechanism can be completely implemented on software to save the investment done in hardware.

This stream cipher algorithm operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plain text to produce the cipher text. The receiver has the same transmission rate as secret key and using the IV, decrypts the message. This mode of transmission works securely when stream cipher key stream is dynamically created. There is no such algorithm in 802.11 standard that prevents the reuse of IV. The Proposed architecture tries to prevent this attack by generating a per-packet key stream as shown in figures 5-1 to 5-9 through signal field, instead of using a single key as secret key for the entire data being transmitted, so that reuse of key streams doesn’t happen.

Since key management was not part of the original 802.11 specification, if an enterprise recognizes the need to change keys often and to make them random, the task is very easy in a large WLAN environment. For example, a large campus may have as many as 15,000 APs. Generating, distributing, loading, and managing keys for an
environment of this size is a significant manageable because of software up gradation.

A summary of the differences between WEP and proposed TKIP Enhancement is demonstrated in the following Table 5-2.

<table>
<thead>
<tr>
<th>Security features</th>
<th>WEP</th>
<th>Enhancement in TKIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Cracked</td>
<td>Fixes WEP flaws</td>
</tr>
<tr>
<td>Key length</td>
<td>40/104 bit keys</td>
<td>128 bit keys</td>
</tr>
<tr>
<td>Key type</td>
<td>Static keys</td>
<td>Dynamic keys</td>
</tr>
<tr>
<td>Key distribution</td>
<td>Manual</td>
<td>Automatic(Signal from PLCP)</td>
</tr>
<tr>
<td>Authentication</td>
<td>WEP Key</td>
<td>Enhanced WEP key</td>
</tr>
</tbody>
</table>

Table 5-2  Comparison of WEP and proposed system

In a nutshell, this research work dynamically changes the IV value to ensure that each frame has a different IV value. Since the IV value is combined with the transmission rate as WEP base key, if the IV value changes for every packet that ensures that every packet is actually encrypted with a different key. This adds more randomness to the encryption process and makes the resulting key stream less predictable. In wireless computing environment, it much harder for the attacker to uncover the original encryption key used.
5.3 SUMMARY

Every mobile station uses the dynamic keys, amount of traffic may not be available to an eavesdropper for analytic attacks. Since the key streams are random and unique, it makes the output of the stream cipher different. Once the base WEP key is changed, new IV/base WEP key pairs are used, and unique packet keys will be generated. The mechanism breaks any one to one relation between TKIP per-packet encryption keys and WEP IV, and the mechanism can be completely implemented on software to save the investment done in hardware. This system also supports the network administrators from the burden of managing static keys and manually rekeying as needed. This firmware update should be implemented in both Access Point Device and Mobile Station (STA) to generate same set of key streams during the time of encryption and decryption.