CHAPTER 3

PROPOSED METHODOLOGY

Proposed Architecture Model for Enhancement to TKIP
Key mixing through Transmission Rate of PLCP

3.1 TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

Temporal Key Integrity Protocol (TKIP) is a suite of algorithms wrapping WEP, to achieve the best security to support the problem design constraints. TKIP is developed to address the vulnerabilities associated with WEP and developed to provide backwards compatibility with WEP to prevent the need to replace all hardware that only supported WEP. TKIP adds new algorithms to WEP:

- A re keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.
- A per-packet key mixing function, to de-correlate the public IVs from weak keys; and
- A new IV sequencing discipline, to remove replay attacks from the attacker’s arsenal;

This research’s main objective is to enhance key mixing mechanisms to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse in TKIP through transmission rate to generate
various pattern of key streams for encrypting and decrypting the transmitted packets.

The security improvement in TKIP is due to the longer key, as well as, using different keys per packet and avoiding key reuse. The proposed enhancement to TKIP frame implies that it creates a new key for each packet significantly reducing the possibility of guessing a key.

**TKIP Frame:** There are a total of 20 octets associated with TKIP in an IEEE 802.11 frame which is indicated in Figure 3-1.

<table>
<thead>
<tr>
<th>Mac Header</th>
<th>IV</th>
<th>Zero Reserved</th>
<th>Ext IV</th>
<th>Key ID</th>
<th>Extended IV</th>
<th>Data</th>
<th>MIC</th>
<th>ICV</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 octets</td>
<td>5 oct</td>
<td>5 bits</td>
<td>1 bit</td>
<td>2 bits</td>
<td>4 octets</td>
<td>0-2312 bits</td>
<td>8 octets</td>
<td>4 octets</td>
<td>4 octets</td>
</tr>
</tbody>
</table>

**Figure 3-1 TKIP Frame**

**IV Sequencing:** TKIP addresses replay attacks by adding a TKIP Sequence Counter (TSC) which prevents reuse of an IV. This is an algorithm associated with TKIP in which a 48-bit counter is employed to ensure a unique IV for each packet. The TSC is broken down into six octets (TSC0 through TSC5) as seen in Figure 3-1. TKIP interprets the IV and extended IV fields of WEP data unit as TKIP Sequence Counter.
(TSC) and as an input to two key mixing functions to produce a per-packet key and IV to feed the WEP encryption algorithm.

TKIP’s per-packet key construction is a feature uniquely necessary to correct WEP’s misuse of RC4. The WEP constructs a per-packet RC4 key by concatenating a base key and the packet IV. The new per-packet key construction, called the TKIP key mixing function, substitutes a transmission signal rate for the WEP base key and constructs the WEP per-packet key. Temporal keys are so named because they have a fixed lifetime and are replaced frequently.

This algorithm also helps prevent denial of service attacks by ensuring that the receiver does not update the TSC until the MIC has been verified after each packet. The final key mixing algorithm protects the Temporal Encryption Key (TEK).

TKIP provides more security with no extra hardware. TKIP uses 48-bits long IV, 64-bit authentication key and 128-bit encryption key. WEP can only accommodate 24-bit IV and maximum of 104-bit encryption key, in comparison with TKIP, the later provides more security against exhaustive key search attacks.

The communication between station (STAs) and the AP utilizes different encryption keys every time a packet is transmitted. These keys are generated from the combination/mixture of a shared base key, sender’s MAC address and packet sequence number, also called TKIP sequence number. Construction of TKIP based on RC4 stream cipher which uses long IV and encryption keys.
TSC requires synchronization between sender and receiver; packets received have to hold a sequence number greater than previously received packets to assure that the packet is not under replay attack. MAC address is used to derive TKIP per-packet encryption key, this is important to guarantee that every STA and AP will generate a different per-packet encryption key, this key will continuously change for every packet in transit as a direct effect of incrementing TSC for every new packet.

Due to MAC addresses differences, every station will generate different set of WEP per packet encryption keys which eliminates key reuse problem in WEP, 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.

There is no direct relation between the IV and the WEP encryption key, because TSC is used to derive the IV and TKIP per-packet encryption keys by means of key mixing functions. When TSC is obtained by attackers, it will have no relation with the TKIP per-packet encryption key so it gives no extra information to the attacker. TSC is initialized by both sender and receiver, when the 128-bit shared key changes, the TSC will reset to some offset value.

3.2 PHYSICAL LAYER CONVERGENCE PROTOCOL(PLCP)

Physical Layer Convergence Protocol(PLCP) preamble which contains the following fields: Synchronization (SYNC) and Start Frame Delimiter (SFD). All 802.11 packets contain a small preamble before the data payload which is sent at a low bit-rate. The preamble contains the
length of the packet, the bit-rate for the data payload, and some parity information calculated over the contents of the preamble. The preamble is sent at 1 megabit in 802.11b.

The PLCP header contains the following fields: signal (SIGNAL), service (SERVICE), length (LENGTH), and CRC-16. TheSYNC field can perform the necessary synchronization operations. The Start Frame Delimiter(SFD) shall be provided to indicate the start of PHY-dependent parameters within the PLCP preamble.

3.3 MULTI RATE SWITCHING:

802.11 specifies a multi rate mechanism in the Physical Layer(PHY) for supporting multiple data rates. 802.11 b specifies 4 data rates from 1 mbps to 11 mbps. 802.11 a/g offers 8 data rates from 6 mbps to 54 mbps. A station selects a transmission rate for every frame that it sends. The rate selected depends on the success of prior transmission.

3.4 REQUIREMENT ANALYSIS

3.4.1 HARDWARE

The proposed work needs the following requirements:

- A 10/100 Mbps Local Area Network device such as a hub or switch
- Ethernet cable with RJ-45 connector.
- A 100-240 V, 50-60 HZ AC power source
• A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above
• Two computers with the TCP/IP protocol installed
• 802.11b-compliant devices, such as the NETGEAR WG511 Wireless Adapter.

**NETGEAR WG102 ProSafe 802.11g Wireless Access Point**

The NETGEAR WG102 ProSafe 802.11g Wireless Access Point is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. The WG102 provides wireless connectivity and interacts with a wireless network interface card via an antenna. Typically, an individual in-building access point provides a maximum connectivity area with about a 300 foot radius. The NETGEAR WG102 ProSafe 802.11g Wireless Access Point can support between 30-50 users simultaneously. The NETGEAR WG102 ProSafe 802.11g Wireless Access Point acts as a bridge between the wired LAN and wireless clients. Further information about NETGEAR WG102 ProSafe 802.11g Wireless Access Point is available in Annexure.

**Lap Top Computer Configuration:**

- Processor: Intel® core i5 250 GHz
- Harddisk: 580 GB
- RAM: 4 GB
- System Type: 64 bit OS
3.4.2 SOFTWARE

OPERATING SYSTEM : Windows 7 home Premium
SIMULATION TOOLS : Mat Lab 7

3.4.3 ASSUMPTIONS

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.

3.5 Architecture Model for Enhancement to TKIP Key mixing through Transmission Rate of PLCP.

TKIP is the economical and feasible solution to WEP problems where it provides more security with no extra hardware. The security improvement in TKIP is due to the longer key and IV lengths used, as well as using different keys per packet and avoiding key reuse. The following Figure 3-2 explains proposed architecture to enhance TKIP frame to update IV to generate dynamic key streams.
Figure 3-2 Architecture Model for proposed Enhancement to TKIP frame through PLCP PPDU frame

There are 8 octets associated with TKIP IV of 802.11 frame. TKIP sequence number is a sequence counter that increments every time a packet is sent, this counter reside in the IV (3 octets) and extended IV (4 octets) fields of WEP data unit. The IV field which includes WEP seed is considered for enhancement to generate dynamic pattern of key streams. Instead of WEP seed, the SIGNAL RATE value from PLCP frame is
assigned to generate dynamic key streams for each transmission. TKIP interprets the IV and extended IV fields of WEP data unit as TKIP Sequence Counter (TSC).

To defeat replays, TKIP reuses the WEP IV field as a packet sequence number. Both transmitter and receiver initialize the packet sequence space to zero whenever new TKIP keys are set, and the transmitter increments the sequence number with each packet it sends. TKIP requires the receiver to enforce proper IV sequencing of arriving packets. TKIP defines a packet as out-of-sequence if its IV is the same or smaller than a previous correctly received MPDU associated with the same encryption key. If an MPDU arrives out of order, then it is considered to be a replay, and the receiver discards it and increments a replay counter.

TKIP’s per-packet key construction is a feature uniquely necessary to correct WEP’s misuse of RC4. WEP constructs a per-packet RC4 key by concatenating a base key and the packet IV. The new per-packet key construction, TKIP key mixing function, substitutes the SIGNAL RATE value from PLCP frame for the WEP base key and constructs the WEP per-packet key to generate dynamic key streams for each transmission.

IEEE 802.11b WLANs support dynamic transmission rate selection to combat adverse wireless channel conditions. Four transmission rates are allowed: 1, 2, 5 and 11 Mbps. The sender of a frame can decide the transmission rate to use based on recent observations of wireless channel conditions (e.g., successful transmissions, missing ACKs, excessive retransmissions). While the multi-rate scheme offers performance advantages, it can suffer from throughput degradation when several
mobile stations share the same physical channel. The AP broadcasts a beacon frame every 100 ms. A mobile station receiving the beacon frames uses the received signal strength to determine the appropriate channel and transmission rate to use.

The PHY exchanges PHY protocol data units (PPDU) that contain PLCP Service Data Units (PSDU). The MAC uses the PHY service, so each MPDU corresponds to a PSDU that is carried in a PPDU. A PMD system, whose function defines the characteristics and method of transmitting and receiving data through a wireless medium between two or more STAs. The most important parts of the physical layer are the modulation techniques and channel coding. The original 802.11 standard specified Direct Sequence Spread Spectrum (DSSS) radios that operate at 1 megabit in the 2.4 gigahertz frequency range. 802.11b added additional higher bit-rates, and 802.11g added bit-rates that use Orthogonal Frequency Division Multiplexing (OFDM). 802.11a allows use of frequencies at 5.8 gigahertz using only the OFDM bit-rates. Each transmission rate (bit-rate) uses a particular modulation to transform a data stream into a sequence of symbols which are encoded by changes in the amplitude, phase, or frequency of an analog signal.

The PHY uses Direct Sequence Spread Spectrum (DSSS) system which operates in the 2.4 GHz ISM band. DSSS modulation builds on the payload data rates of 1, 2, 5 and 11 Mbps. An optional modulation mode known as DSSS-OFDM is also incorporated with payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The 8-bit SIGNAL field indicates to the PHY the modulation that shall be used for transmission (and reception) of the PSDU.
The Key mixing function in TKIP operates in two-phases and substitutes a temporal key (PLCP signal field) for the base key and constructs per-packet key. In this research PLCP signal field is initialized as WEP seed in TKIP frame. For each transmission, a different signal rate is selected by PHY based on the channel condition. So the key mixing functions will be dynamically updated to generate per-packet IV during each transmission. MAC address is also used to derive TKIP per-packet encryption key, this is also important to guarantee that every STA and AP will generate a different per-packet encryption key, this key will continuously change for every packet in transit as a direct effect of incrementing TSC for every new packet. This new key mixing mechanism highlights couple of 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. The following Figure 3-3 shows a block diagram that explains the construction of TKIP per-packet keys.

![Figure 3-3 TKIP Key mixing](image-url)
The key mixing algorithm is broken down into two parts. Phase 1 combines the 802.11 MAC address of the local wireless interface and the temporal key by iteratively XORing each of their bytes, to produce an intermediate key. Stirring the local MAC address into the temporal key in this way causes different stations and access points to generate different intermediate keys. This construction forces the stream of generated per-packet encryption keys to differ at every station. The Phase 1 intermediate key must be computed only when the temporal key is updated.

Phase 2 uses a tiny cipher to encrypt the packet sequence number under the intermediate key, producing a 128-bit per-packet key. In actuality, the first 3 bytes of Phase 2 output corresponds exactly to the WEP IV, and the last 13 to the WEP base key, as existing WEP hardware expects to concatenate a base key (signal rate) to an IV to form the per-packet key. This design accomplishes the effective mixing function, by making it difficult for an adversary to correlate IVs and per-packet keys.

Phase 2 assigns the 8 most significant bits of the counter to the first and second bytes of the WEP IV, and the least significant counter bits to the third IV byte. It then masks off the most significant bit of the second IV byte to prevent the WEP per-packet key concatenation from producing one of the known RC4 weak keys.

There are two major phases in RC4. The first phase is the key setup algorithm (KSA), which establishes a 256-byte array with a permutation of the numbers 0~255. The permutation in the array, or S-box, is established by first initializing the array with the numbers 0~255 in order. The elements in the S-box are then permuted through the
following process. First, a second 256-byte array, or K-box, is filled with the key that repeats as needed to fill the array. Next, the bytes in the S-box are swapped.

Before the processing (encryption/ decryption) starts, the array S is initialized in the following two steps:

1. The 256 bytes array S is initialized. Another temporary array T of similar size is also used during initialization. Array T is populated with the bytes of the key.
   
   for ( i = 0; i < 256; i++)
   {
       S[ i ] = i;
       T[ i ] = K[ i mod KeyLen ] + {Signal rate value from PLCP};
   }
   // key is repeated, if less than 256 bytes
   
2. The array T is used for permutation of the array S. Array T is not required after initialization process.
   
   j = 0;
   for ( i = 0; i < 256; i++)
   {
       j = (j + S[ i ] + T[ i ]) mod 256;
       Swap ( S[ i ], S[ j ]); 
   }

Once the initialization is done, the stream of bytes is encrypted/ decrypted using following procedure:
i = 0;
j = 0;
while (true)
{
i = ( i + 1 ) mod 256;
j = ( j + S[ i ] + S[ j ] ) mod 256;
Swap( S[ i ], S[ j ] );
t = ( S[ i ] + S[ j ] ) mod 256;
k = S[ t ];
}

The values are reorganized continuously as each pseudorandom byte is generated so there is a different permutation of the array each time. Each pseudorandom byte is generated by picking a single value from the permutation based on two index values, i and j , which also change each time. This is explained in Figure 3-4. There are very many permutations of 255 values that can be made. This property of RC4 makes it very powerful . It is amazingly hard to distinguish an RC4 pseudorandom sequence from a real random sequence. RC4 has been studied by many cryptographers and yet the best know method for distinguishing an RC4 stream from true random data requires a continuous sample of 1 GB of the stream before it can reliably decide that the stream was generated by RC4.

The byte k is used as a key to encrypt/ decrypt next byte of the stream. During encryption, k is XORed with the plaintext byte in order to get the cipher text byte, whereas, during decryption, k is XORed with a cipher text byte to get plaintext byte.
As is evident from the logic of the algorithm, RC4 is very safe, and has not been declared broken. Many people have analyzed and studied the algorithm critically, but nobody has found out any short cut to break the cipher with a reasonable key length such as 128 bits. Ideally, if any one bit in the key is changed, then the output key stream should be totally different. Each bit should have a 50% chance of being different from the previous stream as illustrated in Result chapter. Some bits of the key had a bigger effect than others. Since IV is added to the secret Key (signal rate), that leads to changes in IV.

The keys are generated from the combination/mixture of a shared base key, sender’s MAC address and packet sequence number, also called TKIP sequence number. During phase 1 the TKIP mixed Transmit Address and Key (TTAK) are generated by the combination of the TSC which also contains SIGNAL rate, TA, and TEK components. During phase 2 the TTAK is combined with a full TEK and TSC to generate the 128-bit WEP seed. Once the WEP seed is generated, it is run through the RC4 algorithm and the key stream is generated and it is XOR with the data to create the encrypted packet. The communication between STAs and the AP utilizes different encryption keys every time a packet is
transmitted. The following Figure 3-5 explains TKIP encapsulation function.

![Figure 3-5 TKIP Encapsulation](image)

When the station wishes to transmit, the TKIP implementation uses the temporal Michael key to compute the MIC of the source and destination MAC addresses, as well as the MSDU payload. TKIP appends the MIC to the data field, thus extending the packet’s data payload by 8 bytes. Next the 802.11 implementation fragments the MSDU into MPDUs as needed by the ambient environment. Once done, it assigns
each fragment a packet sequence number and employs the key mixing function to create a per-packet encryption key for each, represented as a WEP IV and a base key (SIGNAL RATE).

With the generation of the WEP seed complete, the TKIP packet can be encapsulated with a process that is similar to the WEP encapsulation process with a few additional steps. The system computes and appends the ICV to the data field ICV of each fragment. The encryption consumes the IV and base key, encrypts the data field, including the MIC and ICV, and encodes the IV and the key id of the set of temporal keys into the WEP IV field, completing the encapsulation process. As the WEP seed is run through the RC4 algorithm and the key stream is generated it is combined with the data to create the final packet. The entire MPDU is now protected and ready to transmit.

3.6 SUMMARY

This proposed methodology addresses the most vulnerable aspect of the WEP by dramatically reducing the re-use of keys. The transmission rate specified in the Signal field of physical layer convergence protocol of physical layer has been assigned to IV field of temporal key integrity protocol frame of data link layer in order to generate dynamic keys for producing cipher text. Since IV is random value that changes with every instance of the cipher that is used to add randomness to the output of the cipher.