**CHAPATER 1**

**INTRODUCTION**

A hotspot is a physical location that offers the internet connection over the wireless local area network. The hotspot can be found in any public place, urban area, and etc. Generally, the internet link is established with the help hotspots using Wi-Fi technology and a strong signal selection mechanism in a certain area. WPA and WPA2 are the most popular protocol for authenticating users in the wireless environment. Wireless Protected Access or WPA has been developed according to IEEE 802.11 standard to remove the drawbacks of WEP. However, it is too simple to break its security protection. That is why WPA2 has been introduced. It uses the combination of AES (Advanced Encryption Standard), Counter Mode CBC-MAC Protocol (CCMP) and Counter Mode Cipher Block Chaining Message Authentication Code Protocol. It offers strong authentication and data security during and after establishing a connection. However, it is too complex to implement for small as well as tiny devices which comprise low storage and less processing capacity. Therefore, it makes the data transfer process slow due to its high time complexity.

we have developed, implemented and evaluated a novel hotspot selection Protocol specification taking QoE demands and fairness metrics into account. It works with the intelligent user hot-spot allocation to act as cells within a super-cell . A group of nodes is chosen to act as cluster-heads for a network of underlying nodes. Here, the cluster heads and their associated slave nodes are chosen for avoiding the overlap of clusters. At the same time, it will offer strong authentication and data protection with low time and space overheads.

**1.1 PROPOSED METHOD**

The hotspot selection and authentication of source as well as users during the establishment of any connection through hotspot are the big and legitimate issues in wireless network architecture. However, the exiting protocols are unable to address these both issues in a combinatorial way. Hence, we have panned as well as designed a new protocol to address these both issues.

Basically, the proposed technique has two parts. The first part includes some assumptions about required parameter which will be used to define the hotspot selection process. The second part defines the selection and validation process of a hotspot in any network area. Both components are further described in detail at the bellow sub sections.

Assumption:

* Let L be the total number of highly demand cluster i.e. where the load of traffic is higher than the normal.
* M is the total number of candidate hotspots, must be connected with at least one demand cluster.
* Let be the signal strength of hot spot *j* in any demand cluster *i.*
* Let  be the location of demand cluster *i.*
* Let  be the average traffic load of any demand cluster *i*.
* Let be a binary variable. When its value is 1, the demand will be assigned to Hotspot
* Let be bandwidth of any Hotspot .
* Let be congestion factor of any Hotspot

Selection Technique

* Scan all the hotspot in a particular location.
* Divide the area into certain number of cluster, based on hotspot availability such that a cluster should have connection with at least one hotspot.
* Calculate the congestion level of each hotspot by the following formula

Where,

Here becomes 1 when the signal strength reaches to the predefined threshold value.

* After determining the congestion level of each hot spot with the step-3, select the hotspot with smallest congestion level.
* Log in with the lowest congested hotspot using required user id and password. If the log in fails, tries other available low congested hot spot.
* After successful logging in through a hotspot, the server will return an AES encrypted affirmation to the client. The client then decrypts this encrypted message and checks the validation information. If within a certain period of time, the client does not get any acknowledgement, it disestablishes the connection as well as finds other low congested hotspot and repeats steps 5 and 6
* A secure connection has been established after the two- way validation. At the same time, the user can transfer or get data to or from the server. The planned protocol uses AES encryption technique to offer strong and less complex authentication mechanism as well as to resolve the limitations of WPA and WPA2. Before establishing a connection, client sends a AES encrypted message and secret key to the hotspot server. The server decrypts the secret message to examine authenticity of a client and sends an acknowledgement to the client. Thus two ways authentication process is being executed and the connection gets established.

Generally, monitoring as well as arrangement of both data link layer and the network component are controlled by wpa\_suppliment tool (available in Linux) and DHCP client module. Disconnection of any hotspot is mostly observed by communicating with Linux kernel with the help of a datagram oriented Netlink Socket. Hotspots monitor system helps to scan the network channel, creates a sorted list of possible candidate hotspots and finally, it helps to configure using DHCP. We have considered the scenario of video conferencing to measure the performance of the proposed protocol. The required specifications for performing this test have been shown at Table-1.

|  |  |
| --- | --- |
| **Required Parameters** | **Specifications** |
| Ethernet inter-frame overhead | 20 Bytes |
| Voice Payload | 20 Bytes |
| UDP header size | 8 Bytes |
| Overhead per call | 39200 bps |
| Max warless channel capacity | 11 Mbps |
| Average Traffic Load | 1040 kbps |
| Minimum band width requires | 2-5 Mbps |

**Some Important Definition**

Few important parameters have been defined in this sub- section to analyze the performances of planned protocol at the Result Analysis section by using them.

* Transmission Delay(DT):In packet switching, the transmission delay is the quantity of essential time to impulse all packets into a transportation channel. The transmission delay can be caused by channel congestion and data speed of the communication linkage.

Where, *N* is bit-number and *R* is transmission rate.

* *Jitter:* Jitter can be defined as the dislocation of a signal pulsation for any extraordinary rate of that particular digital signal. Conventionally, if Jitter is high, then the communication link is considered as weak. If the clock frequency of any signal is and the phase noise of the signal is for a time period of *t,* then the Jitter for each cycle can be represented as,
* *Data Loss(DL):* Data loss (DL) is the losses of transmitteddata in terms of packets during the transmission. Packet loss or corruption occurs due to network failure, high delay, channel congestion and other reasons. Data loss may cause noticeable effects in digital communication. The data loss can be measured as,
* *Traffic Load:* Traffic load in the mobile communication is the amount of total calls in a certain time period. In our context, traffic load represents the total number of nodes connected through a particular channel. Traffic load can be evaluated in terms of Erlang. The Erlang unit is basically used to measure the telecommunication traffic and is represented by the symbol . The traffic load in terms of Erlang can be stated as,

Where, is average traffic load in terms of Erlang, is the total amount of data transfer per unit time, and *T* is average packet transmission time.

* Avalanche Effect: In any cryptography based authentication system Avalanche Effect calculates the effect of bit filliping over the complete transmitted message. The bit flipping occurred due to various security attacks or limitation of transmission System. Avalanche Effect determines the strength of an encryption technique to provide data security. The Avalanche Effect can be calculated as,
* *Entropy:* As per the Information Theory, entropy is used to calculate the ambiguity connected with a random variable. Furthermore, it can determine the strength of any security technique such as cryptography to protect distinct data security challenges. Entropy, offered by any cryptography technique can be defined as,

The above equation signifies the probability of symbol. The ideal *Entropy* value for an encrypted message should be 8. Therefore, a cryptography based authentication system is said to be strong if it produces the entropy values closer to 8 or vice versa.

As per the first objective, our planned protocol finds the highest signal strength for communication which has been decided by measuring the Jitter with the help of Equation (3) and plotted in the following Fig.3

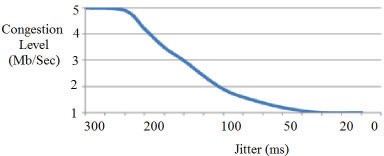


Fig.3: Jitter of signal according to the congestion level.

In the Fig.3 the jitters of different communication links in a certain time span are calculated and plotted according to the congestion level. The proposed protocol selects strongest signal with the lowest jitter. Thus it fulfills the first objective.

The proposed protocol calculates the transmission delay with the help of Equation 2 to find the lowest congested hotspot. The traffic delay belongs to any Hotspot have been calculated in terms of Erlang using Equation 5. The transmission delay offered by any hotspot and the traffic load of different available hotspot are calculated and shown in Fig.4 and Table-2.

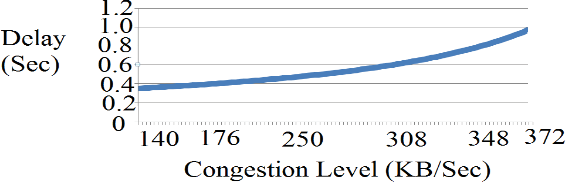


Fig.4: Transmission delay offered by different hotspots

TABLE 2. Traffic delay offered by various Hotspot.

|  |  |
| --- | --- |
| **(Traffic Load)Erlang** | **Congestion (Mb/Sec)** |
| 28.64583 | 0.034091 |
| 28.56731 | 0.068369 |
| 28.48921 | 0.068557 |
| 28.41154 | 0.068744 |
| 28.33429 | 0.034466 |
| 28.25746 | 0.034559 |
| 28.18104 | 0.10396 |
| 28.10504 | 0.069494 |
| 28.02945 | 0.139362 |
| 27.95426 | 0.139737 |
| 27.87947 | 0.105084 |
| 27.80509 | 0.105365 |
| 27.7311 | 0.140862 |
| 27.6575 | 0.105927 |
| 27.58429 | 0.070806 |
| 27.51147 | 0.070993 |
| 27.43903 | 0.071181 |
| 27.36697 | 0.071368 |
| 27.29529 | 0.107333 |
| 27.22399 | 0.071743 |

Fig.5: Data loss offered by the proposed protocol

Fig.4 shows that our proposed protocol is able to calculate lowest delay, produced by the available hotspots during the establishment of connections. Taable-2 reflects that the proposed protocol has potentiality to analyze the traffic load of a particular hotspot in terms of calculating the Erlang value.

The data loss occurs in term of packet loss due to the high transmission delay and traffic load. Sometime various security attacks can also be the causes of data loss during the transmission. The potentiality to prevent the data loss, offered by the proposed protocol has been calculated for various hotspots based on their congestion level with the help of Equation-4 and shown in Fig.5.

Figure-5 shows that our proposed technique offered very low data loss in every occasion. Therefore, we can claim from the Fig.5, Table-2 and Fig.5 that our planned system is competent to improve the data transfer rate by selecting the lowest congested hotspot and it is also effective to diminish the data loss in the course of transportation. Thus we have achieved our second objective.

Simultaneously, the potentiality to overcome various security attacks has been determined by calculating the Avalanche Effect and the Entropy value with the help of Equation-6 and Equation-7 and shown in Table-3.

TABLE 3. AE AND ENTROPY VALUES FOR CRYPTOGRAPHY TECH.

|  |  |  |
| --- | --- | --- |
| Security Techniques | Avalanche  Effect (In %) | Entropy  Values |
| AES | 65.2 | 7.73 |
| Triple DES | 64.3 | 7.53 |
| 3-DES | 62.2 | 7.67 |
| Blowfish | 59.2 | 7.52 |
| RSA | 61.6 | 7.51 |

Above Table-3 shows that AES offers higher Avalanche Effect and Entropy Values than other existing. So, AES has higher potential to prevent various security attacks than others. As a consequence, AES in our proposed protocol offers a strong validation system for hotspot authentication. Thus our third objective is fulfilled.