VISVESVARAYA TECHNOLOGICAL UNIVERSITY

JNANA SANGAMA, BELAGAVI-590018

A Project Report

on

Service Period Bandwidth Allocation using Modified Round Robin and RSNA Authentication for 802.11ad Infrastructure

Submitted in partial fulfillment of the requirements
for the award of the degree of

Bachelor of Engineering
in
Computer Science and Engineering
by

SUMIT KUMAR	**1BG12CS101**
VENKATESH PRASAD S	**1BG12CS117**
VINAY B	**1BG12CS121**
YOGANAND G K	**1BG12CS125**

Under the Guidance of

Internal Guide
Dr.Divyashree BA
Professor
Dept. of CSE
B.N.M.I.T

External Guide
Mr.Sathish Srinivasan
Software Engineer
Asarva Chips & Technologies
Kasturba Road

Vidyaya Amrutham Ashnuthe

B.N.M. Institute of Technology

12th Main, 27th Cross, Banashankari IInd Stage, Bangalore 560 070.

Department of Computer Science and Engineering

2015– 2016

B.N.M. Institute of Technology

12th Main, 27th Cross, Banashankari IInd Stage, Bangalore 560 070.

Department of Computer Science and Engineering

Vidyaya Amrutham Ashnuthe

CERTIFICATE

Certified that the project work entitled **Service Period Bandwidth Allocation using Modified Round Robin and Implementation of RSNA Authentication for 802.11ad Infrastructure** is a bona fide work carried out by

1. SUMIT KUMAR	**1BG12CS101**
2. VENKATESH PRASAD S	**1BG12CS117**
3. VINAY B	**1BG12CS121**
4. YOGANAND G K	**1BG12CS125**

in partial fulfilment for the award of Bachelor of Engineering in Computer Science and Engineering degree of Visveswaraya Technological University, Belagavi during the year 2015-2016. It is certified that all corrections/suggestions indicated for the internal assessment have been incorporated in the report deposited in the departmental library. The report has been approved as it satisfies the academic requirements in respect of project work prescribed for the said degree.

Dr. Divyashree B A	**Dr. Sahana D Gowda**	**Dr.Krishnamurthy G N**
Professor	Professor and Head	Principal
Dept. of CSE	Dept. of CSE	B.N.M.I.T
B.N.M.I.T	B.N.M.I.T	

Name of the Examiners	**Signature with date**
1	
2	

priority queue until it is empty, and then moves to the next highest priority queue. This mechanism could cause bandwidth starvation for the low priority QoS classes.

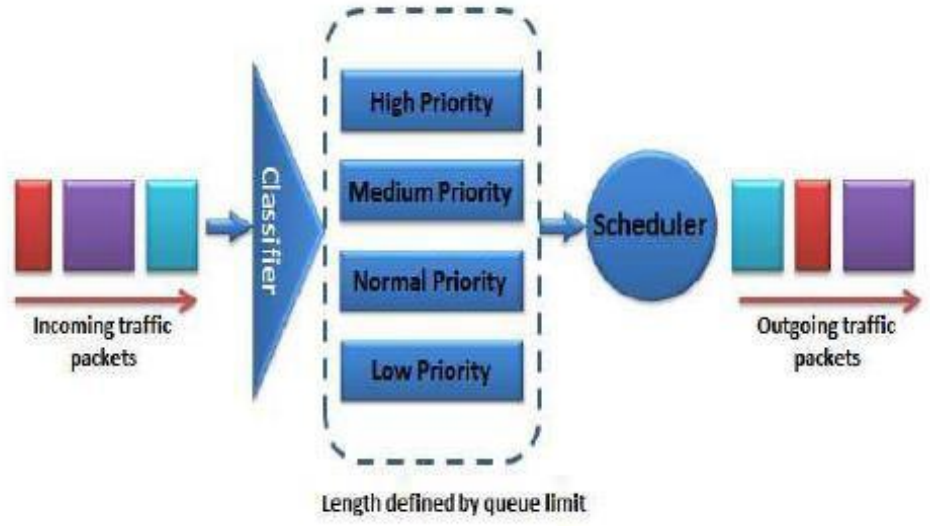

Figure 4.2: Strict Priority Queuing

As depicted in the Figure 4.2, the algorithm services the highest priority queue until it is empty, after which, it moves to the next highest priority queue. Thus, strict-priority algorithm is not suitable for most of the wireless network applications. This is because there is no compensation for inadequate bandwidth. Also this technique is only appropriate for low-bandwidth serial lines that currently uses static configuration which does not automatically adapt to changing network requirements. Finally, this process may result in bandwidth starvation for the low priority QoS classes whereby the packets may not even get forwarded and no guarantee is offered to one flow.

4.2 PROPOSED SYSTEM

Implementation of a Robust Security Network (RSNA) for authentication of stations by the Access Point and a modified version of the Round-Robin network scheduling algorithm to efficiently allocate the available bandwidth and maximize the bandwidth utilization.

4.2.1 RSNA AES-GCM Protocol

AES-GCM protocol provides security to the data that is being transferred between the access point and the station and vice-verse.

Galois/Counter Mode(GCM)is a block cipher mode of operation that uses

hence less processing power which results in less delay.

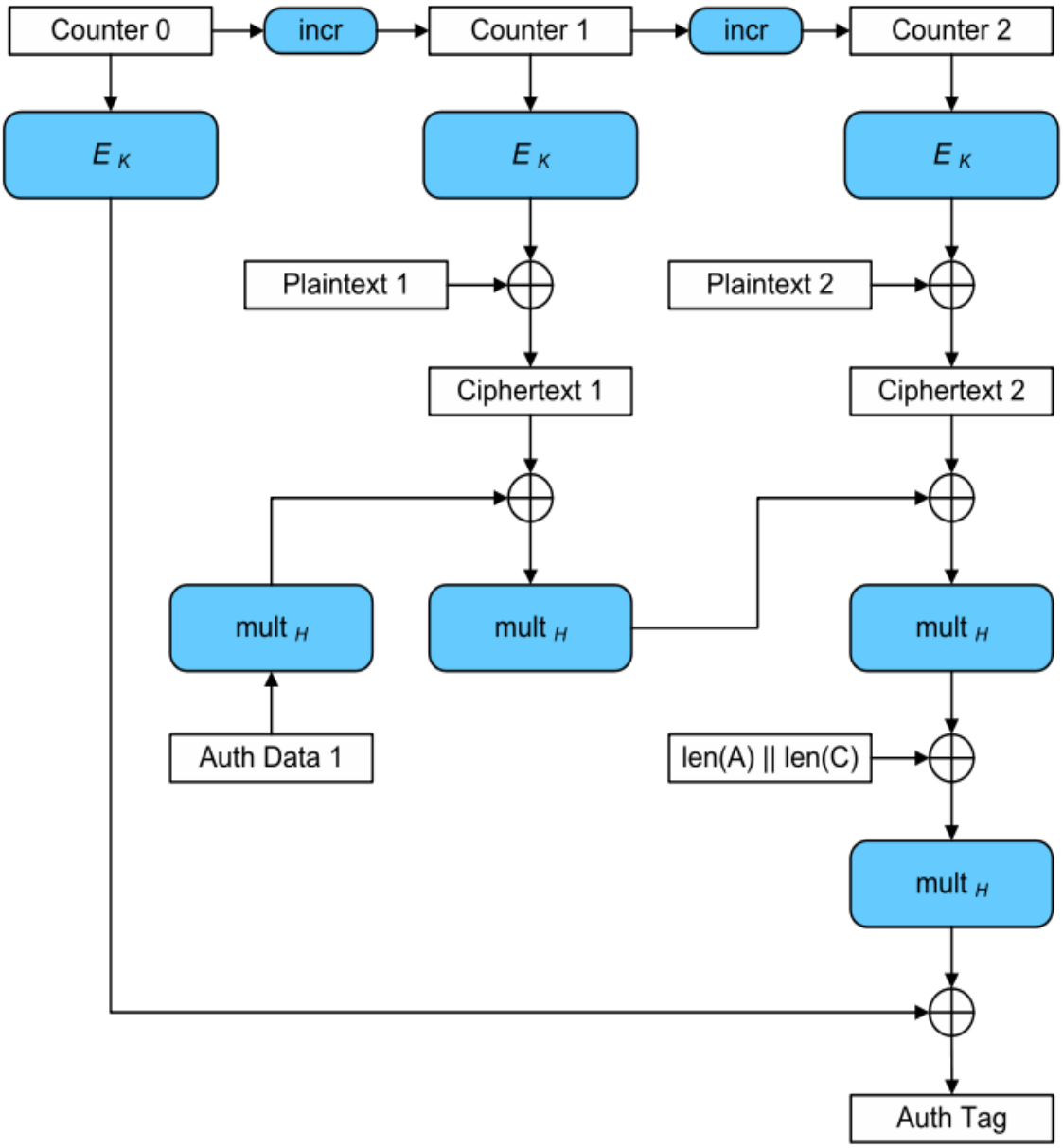

Figure 4.3: GCMP Process

Weighted round robin scheduling method to provide a better servicing method for the access point to service the requests from various stations.

4.2.2 Weighted Round Robin Scheduling

In weighted round robin scheduling, packets are categorized into different service classes and then assigned to a queue that can be assigned different percentage of bandwidth and served based on Round Robin order. This algorithm addresses the problem of

starvation by guarantees that all service classes have the ability to access at least some configured amount of network bandwidth.

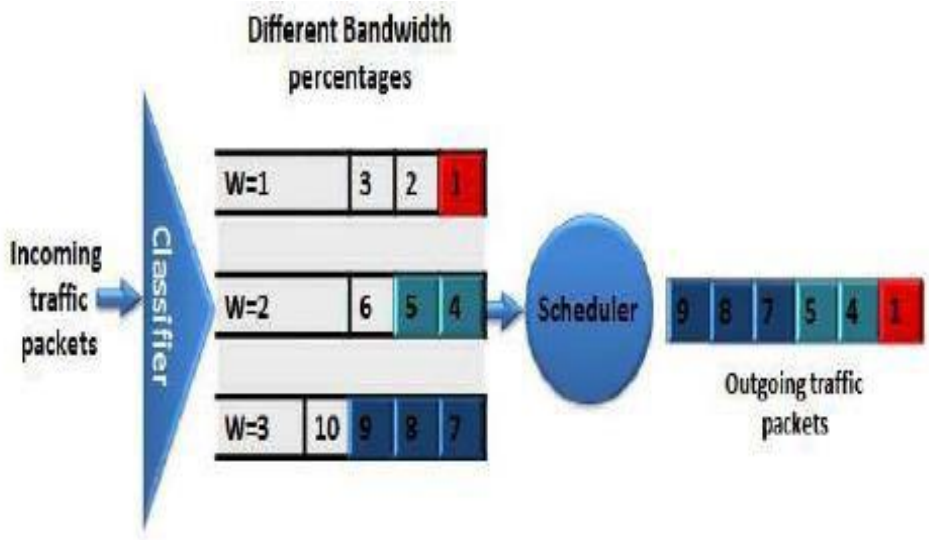

Figure 4.4: Weighted Round Robin Scheduling

As depicted in the Figure 4.4, the packets are first classified into various service classes and then assigned a queue that can be assigned a different percentage of bandwidth and is serviced in round robin order. WRR ensures that all service classes have access to at least some configured amount of network bandwidth to avoid bandwidth starvation. In order to provide the correct percentage of bandwidth to each class all of the packets in tall queues are of same size. The weights of individual classes of priority depends upon the number of packets that dynamically arrive as part of the traffic. The de-queueing of the packets is done based on the computed weights.

6.2 Generate the required keys

The data exchange between the access point and service station happens using keys. The keys include Pairwise Master Key(PTK) and a Group Temporal Key(GTK).

The PTK is generated by both access point and the service station using the ANonce and SNonce. Along with these it also requires the MAC addresses of both AP and STAs. The below function shows the generation of PTK.

PTK = EAPOL-PRF(PMK, ANonce, SNonce, AP-Mac-address, STA-Mac-address) where PMK->pair-wise master key,

ANonce => nonce generated by AP

SNonce => nonce generated by STA

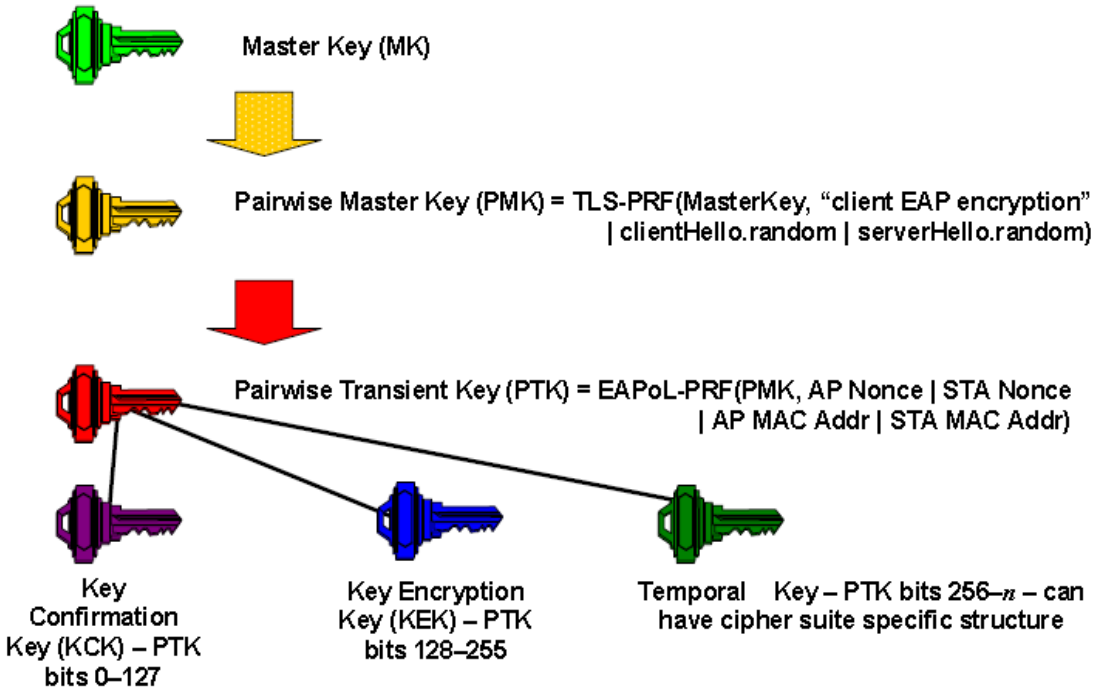

Figure 6.4: Key Hierarchy

The Figure 6.4 shows the Key Hierarchy which shows the keys involved in the generation of Pairwise Transient Key. Master key is used to generate Pairwise Master Key and which in turn is used to generate Pairwise Transient Key. Pairwise Transient Key consist of three different keys Key Confirmation Key (KCK), Key Encryption Key (KEK) and Temporal Key (TK). These keys is generated when a client establishes a secure connection with the server. These keys are generated uniquely for each session which provides more secure communication.

Chapter 8

RESULTS

By using RSNA, the key frames transferred are secure and their integrity is properly assessed (i.e if the data is corrupted or modified by external factors the packet is identified and dropped).

The authentication is a success or a failure depending on the data entered by the STA, in any case the STA cannot receive bandwidth without a success for authentication.

Bandwidth allocation is tested for all possible combinations of requests put forth by the STAs and the effectiveness of the algorithm is realized.

Fair allocation of bandwidth to all requests and its types is the key feature of the algorithm.

8.1 RSNA Authentication

The following snapshots demonstrate the RSNA authentication process:

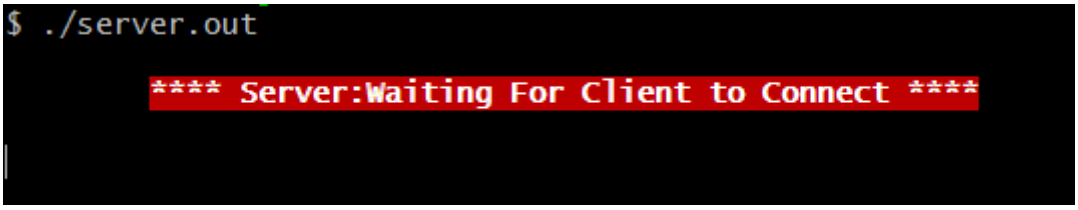

Figure 8.1: Server waiting for a client to connect

Figure 8.1 shows an active server. The server waits indefinitely until any client establishes a connection with it.

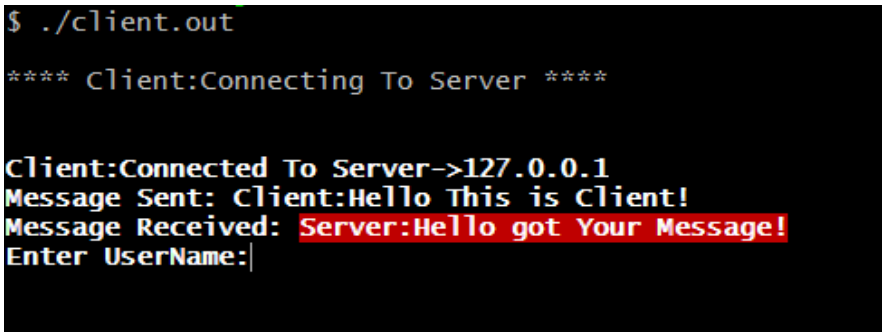

Figure 8.2: Client connects to the server

Figure 8.2 shows client connection establishment. The client establishes a connection with the server. The server then requests for a username and a password for authorization.

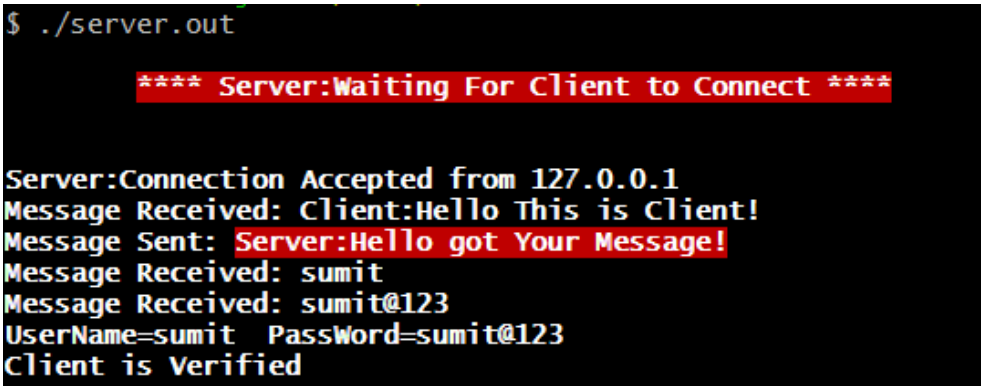

Figure 8.3: The server verifies the client

Figure 8.3 shows the client credential verification by the server. The client sends the credentials to the server. The server verifies the username and password. If it comes out to be a valid user, then the process continues. Else, the process stops.

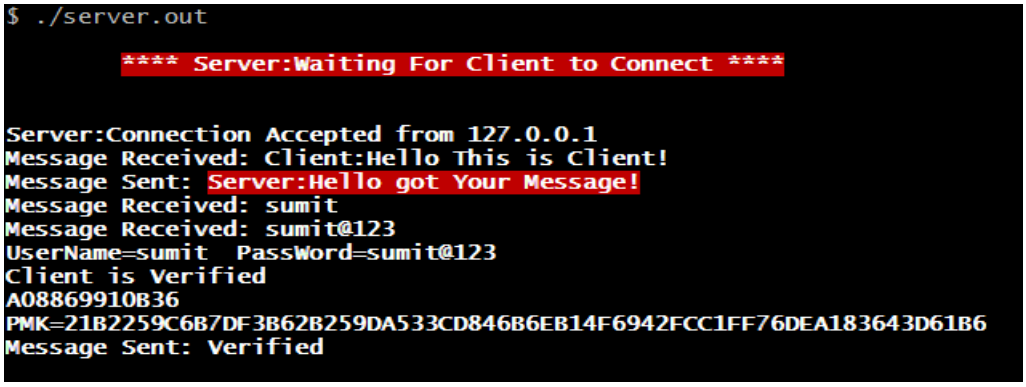

Figure 8.4: Unique PMK for each Client-Server pair

Figure 8.4 shows the PMK generation for every connected client. After the client has been verified, the server sends a Pairwise Master Key (PMK) which is unique for every client-server pair.

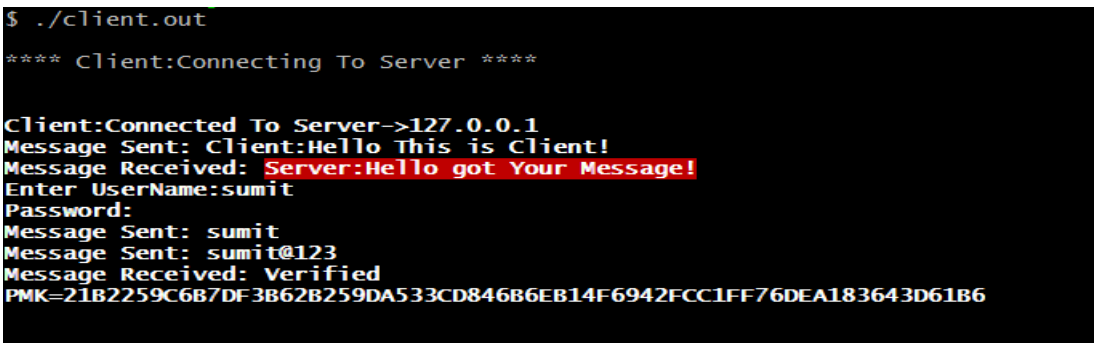

Figure 8.5: Client receives the PMK

Figure 8.5 shows that the client is verified by the AP and the PMK is assigned to the client.

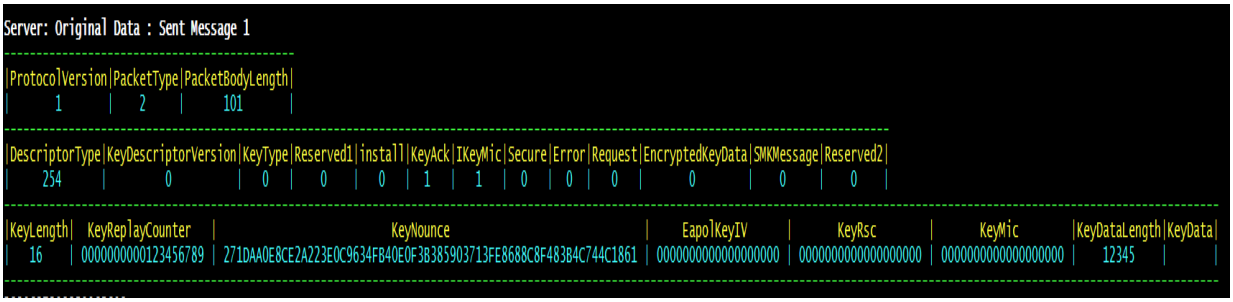

Figure 8.6: Server sends Message 1

Figure 8.6 shows that the server creates ANonce and KeyReplayCounter and the message is transmitted to the client.

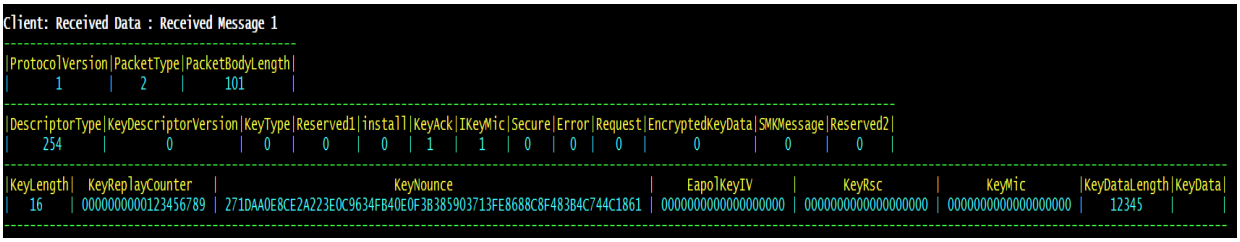

Figure 8.7: Client receives Message 1

Figure 8.7 shows that the client receives the ANonce and KeyReplayCounter from the AP and client generates PTK using ANonce and SNonce.

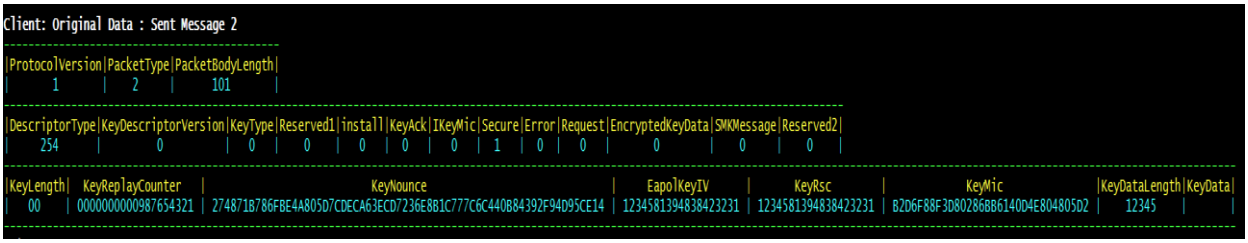

Figure 8.8: Client sends Message 2

Figure 8.8 shows that the client send the SNonce, KeyReplayCounter and KeyMic. KeyMic is created using KCK.

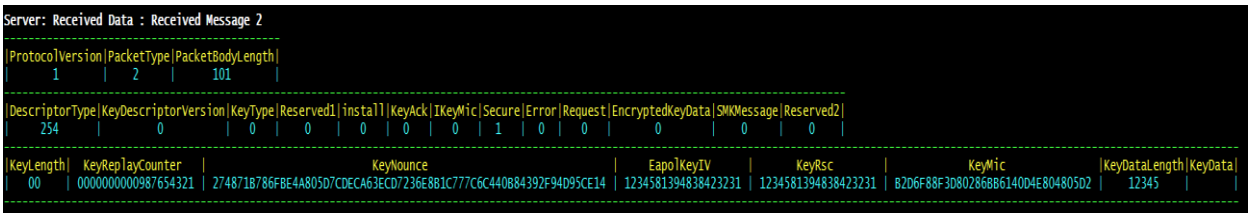

Figure 8.9: Server receives Message 2

Figure 8.9 shows that the AP receives the SNonce, KeyReplayCounter and KeyMic. Ap Verifies the KeyMic and the Message is accepted. And it generates PTK using SNonce and ANonce.

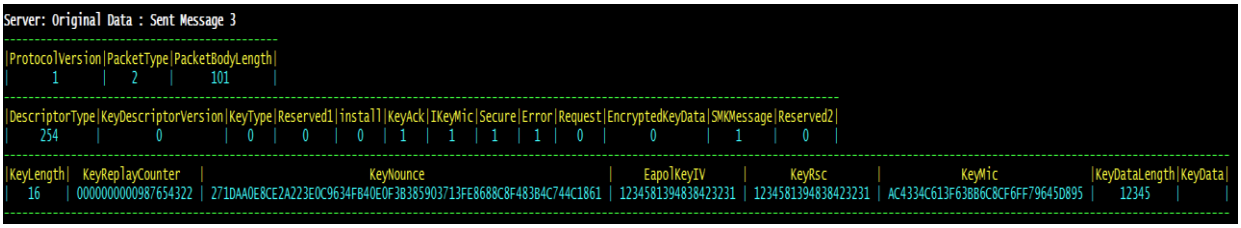

Figure 8.10: Server sends Message 3

Figure 8.10 shows that the AP send the KeyMic and KeyReplayCounter to the client.

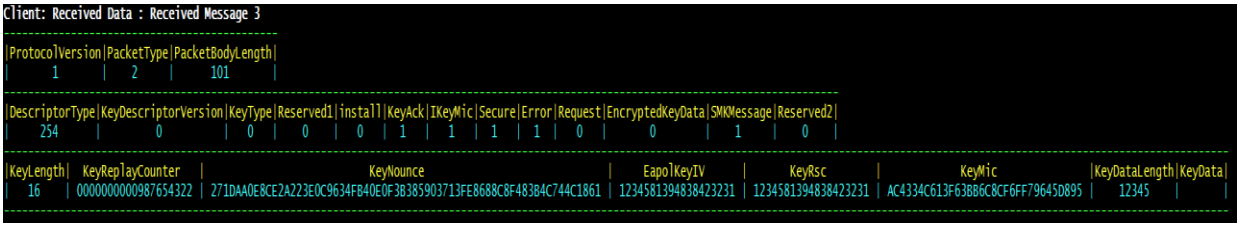

Figure 8.11: Client receives Message 3

Figure 8.11 shows that the client receives the KeyReplayCounter and KeyMic and Verifies the Message using KeyMic and checks for duplicate message using the KeyReplayCounter.

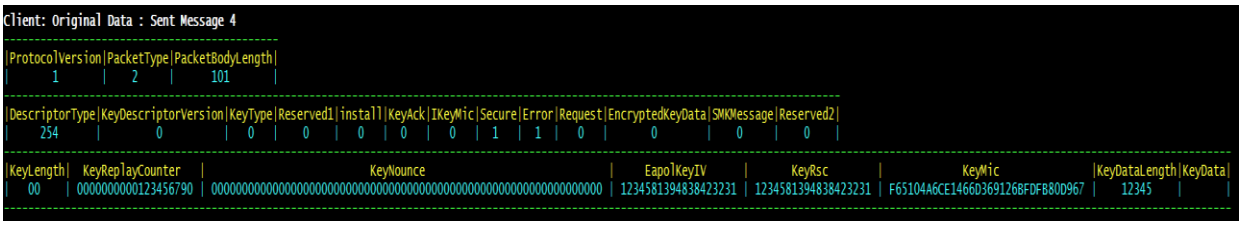

Figure 8.12: Client sends Message 4

Figure 8.12 shows that the client sends the KeyReplayCounter and KeyMic to the AP.

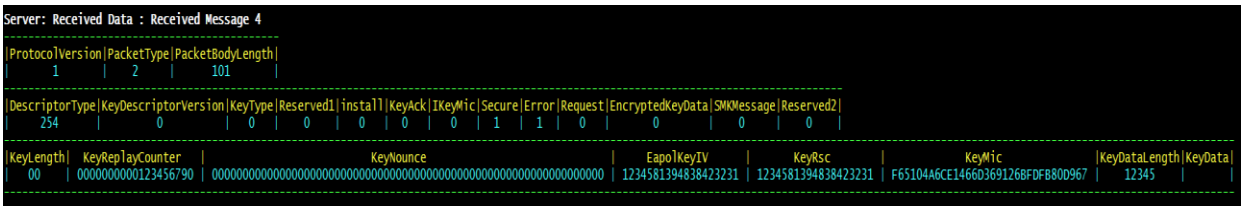

Figure 8.13: Server receives Message 4

Figure 8.13 shows that the AP receives the KeyReplayCounter and KeyMic. KeyMic Verifies the Message and KeyReplayCounter checks for duplicate message.

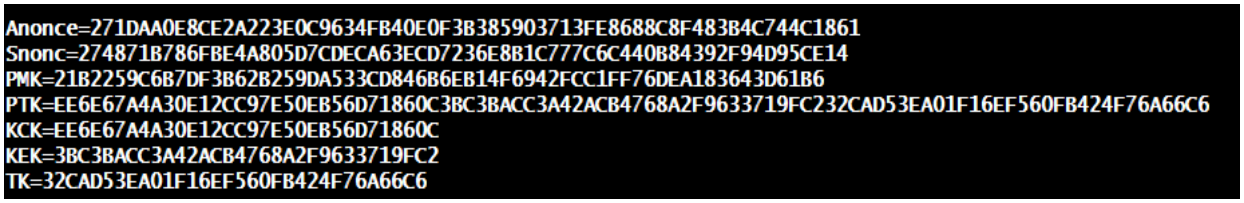

Figure 8.14: Server Exchanged Information

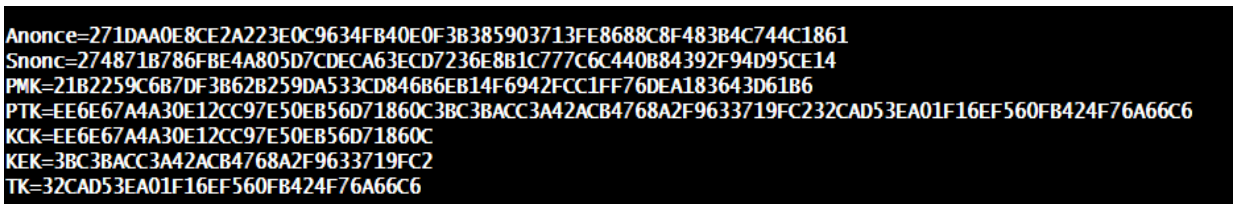

Figure 8.15: Client Exchanged Information

Figure 8.14 and 8.15 shows that the server and client Exchanged information respectively and both server and client have the same pair of keys which allows them to encrypt and decrypt the message.

8.2 Bandwidth Allocation

The following figures demonstrate the working of the Modified Round Robin Service Period Bandwidth Allocation:

Figure 8.16 shows the generation of requests by the client. It is assumed that the maximum available bandwidth is 100MB, the client generates random number of requests of four types of services namely VoIP, Video, Best Effort and Background. The type of service is indicated by the **Queue Index,** and the amount of bandwidth needed is indicated by **BW**.

```
$ ./a.exe
1. Manual Input
2. Generate Randomly
2
Generating Requests:
BW      Queue Index
68      3
47      2
84      3
99      4
90      4
100     1
18      3
44      1
14      2
44      4
84      4
94      3
48      1
44      1
60      2
45      3
The requests have been queued
```

Figure 8.16: Random Request Generation by a client

```
Queue 1 : VoIP
100.0   44.0    48.0    44.0

Queue 2 : Video
47.0    14.0    60.0

Queue 3 : Best Effort
68.0    84.0    18.0    94.0    45.0

Queue 4 : Background
99.0    90.0    44.0    84.0
```

Figure 8.17: Queueing of requests

Figure 8.17 shows the queueing of the generated requests in four different priority queues. The server after collecting the requests from the clients, puts the requests into different priority queues based on the type of service. Queue 1 which is the highest priority queue contains VoIP requests. Queue 2 contains Video requests. Queue 3 and Queue 4 contain Best Effort and Background requests respectively.

Figure 8.18 shows the computation of the allocation factor. After queueing the requests, the server computes the allocation factor which is the ratio of the sum of all requests by all clients to the maximum available bandwidth. Using the allocation factor, the server then computes a fairness factor which serves as weight. The requests are serviced based on the fairness factor of each service type.

Figure 8.18: Allocation Factor computation and Bandwidth allocation

Figure 8.19 shows the Round Robin Bandwidth Allocation. After computing the allocation factor and the fairness factors, the server starts the bandwidth allocation in a round robin fashion. This process happens for multiple cycles until the entire requested amount of bandwidth has been provided. The allocation factor and the fairness factors are computed for each cycle. In case the sum of all requests made is less than the maximum available bandwidth, then the allocation factor will be less than 1 and there will be no need to compute the fairness factors, and hence the entire bandwidth requests can be granted.

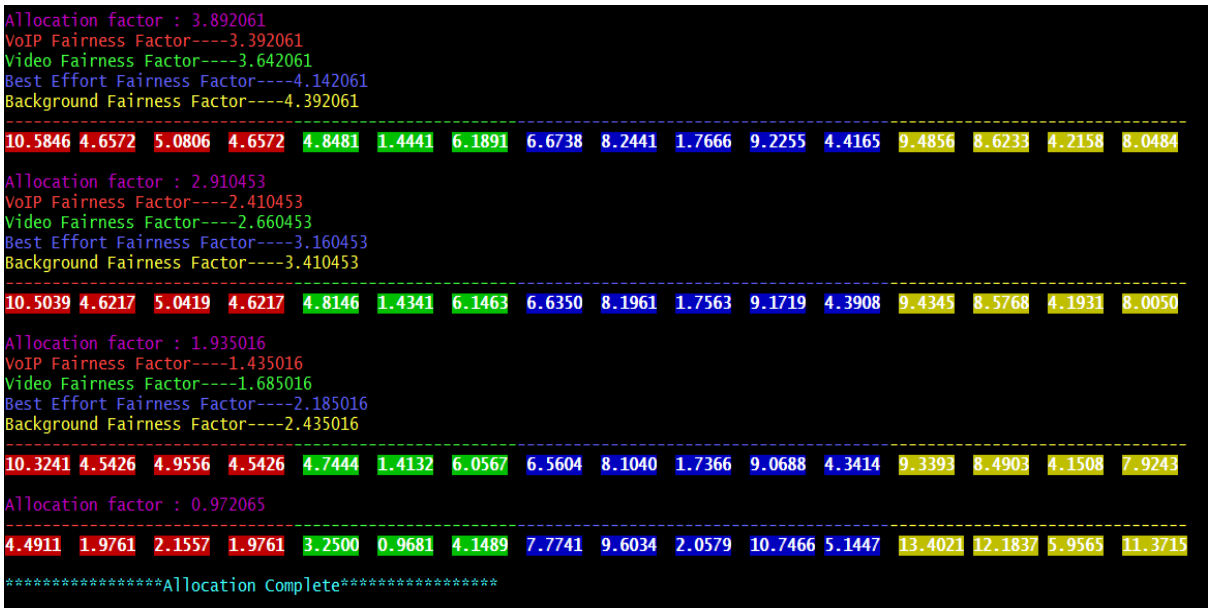

Figure 8.19: Round Robin Bandwidth Allocation