CHAPTER 4

SECURED EFFICIENT FAST HANDOVER MULTIHOMING BASED NEMO+

4.1 INTRODUCTION

Multihoming concept is used to establish Always Best Connected Network in a wireless environment under multi access situations. The multihomed network node usually includes many addresses to access the internet through multiple path networks so that if the current network path fails, it can directly switch to another network path which is active (Ryu et al. 2014). This chapter focuses on the new methodology called Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) that improves the seamless connectivity thereby reducing delay, packet loss and improve the security mechanism in multi-homing environment.

The EFNEMO+ method is improved and extended by adding features that supports multi-homed environment. The proposed Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) mechanism is introduced in multihomed mobility configuration based on flow binding to access the destination network from multiple networks to predict the handover process by accessing the information on actual location and previously recorded context data. Public Key Cryptography method provides a secure acknowledgement before handover process executed; the acknowledgement is encrypted by way of digital signature.
4.2 MULTIHOMING

Multihoming method refers to one network end node accesses to the internet uses multiple network paths to accesses the internet, it resilient the fault in a network. In addition to provide consistent access to the network, EFNEMO+ utilizes multihoming technique. It implements multihoming by using geographical location information of the nodes of the network and gathers the recorded context data to access the network parameter. These information help EFNEMO+ protocol to handle the handovers proactively to access the networks. This protocol focuses on the use of redundant network links for the use of external connectivity. A multihomed node is physically attached over multiple network interfaces that have different IP addresses and might be attached to the same otherwise with the different networks also it uses the similar or different access technologies. In IPv6, each network interface can have several IP addresses. Multiple Care-of Addresses Registration (MCoA) is introduced to the Mobile IPv6 protocol relation. Using MCoA the mobile nodes or routers get connected to multiple access networks concurrently; it is currently possible to improve the network redundancy, handover latency and performs policy based routing even in multi-access environments.

4.3 PROPOSED SECURED EFFICIENT FAST HANDOVER MULTIHOMING BASED NEMO+

The Secured Efficient Fast Handover Multihoming Based NEMO+ utilizes multihoming technique when the current working path fails. It can change its address immediately and another network path communicates with the network. It uses network end node that access the internet which uses multiple network paths to connect the network. These handovers are handled blind, as no network context information is available during the processing
stage. The reactive behavior is used in this process. In order to provide the seamless connectivity to the MR the predictive policy exchange message is used and it will avoid delay of packet and loss during handover. The Elliptic Curve Digital Signature Algorithm (ECDSA) used in this work that provides protection for the BU messages. Private Key-based Binding Update (PKBU) protocol is used to provide the security effectively. This protocol helps to effectively protect the FBU message against attacks by adversary.

The proposed Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) algorithm with multi-homed mobility configuration depends on flow binding to access the target network from multiple networks. It predicts the handover using the actual location information and already recorded context data.

4.3.1 Predictive handover technique

There are three main functions for predictive handover technique.

- Access Network Prediction (ANP)
- MR’s Handover Manager (HM-MR)
- Home Agent (HM-HA)

Access Network Prediction

Depending on the updated network database, the positions, current, speed, the ANP afford network parameter prediction to HM-MR and it have some functionality to maintain the network access database, transfer the prediction message to HM-MR and from GNSS receiver. It reads GNSS message and process the network capacity which are from HM-MR segment. It must provide the stability of update about the movement of the MR.
MRs Handover Manager

The Access Network Prediction sends the predictive message to HM-MR; it denotes these messages in XML format. Later it integrates the GNSS messages using latitude and longitude values which are multiplied with 10,000 and are rounded off to the nearest integer value to avoid the network database from explosion. It fixes the limited space for prediction called raster points.

Home Agent

Based on the host node where they rely on, HM-MR divides into two processes prediction process and handover policies. Handover policies measure the information regarding the status of channel and during the MR movements it will maintains the parameters towards availability of network access. The decision algorithm is used to the scale the parameters are IPv6 prefix information, Receive signal strength indicator of UMTS, Basic ServiceSet Indicator (BSSI) and Signal to Noise Ratio of WLAN. Simultaneously HM-MR prepares predictive handover process based on the XML message. After TD and NINA message from MR it handles the RRH message in a timed modus and it interacts indirectly with NEMO NCoA. This is achieved by applying Predictive Policy Exchange that update about future handovers in Mobile router to HM-MA.

When HM-MA initiates the handover, the information is received periodically about network access that is needed for handover and decision algorithm selects the destination network when future handover are near. HM-MA selects the highest priority WLAN among another WLANs and 3g/UMTS as destination network. The WLAN is considered as highest priority when it has best SNR value. Predictive policy exchange method in the
HA has instance for predictive, timed and flow binding to interact HA with HA-MA module. Before the actual handover taken place, HA informs about the network prefix, timing, and changes that happens in the flow binding are scheduled and executed.

After the destination network selected to MR, it allow destination network to pass over in flow binding sub modules, in turn the signal between HA and MR are handled by these sub modules. The destination network is selected and predictions on layer1/layer2/layer3 are prepared before executing the timed and synchronized policy exchange for burrow between MR and HA. The execution of predictions the policy exchange commands of HA-MR and HM-HA are done in same time in the GNSS i.e. the traffic in the EFNEMO+ are redirected to the new network defined in new MCoA. This result in the loss of packets and other QoS are unnoticed in the functional path, the predictive policy exchange message that switches the flow of packets in a timed manner and even if failures happens in the active access network, it ensure the seamless connectivity by selecting the next highest priority WLAN. Delay and loss of packets are controlled in multihoming handover.

When HA perform Handover with MCoA, first it discover the MR and routes by using TD, NINA and RRH protocols. In the inactive interface HM establish new binding when it connects to new network. After current node and new access network is connected, a burrow is established between MR and HA. When the handover operation is performed using flow binding it moves from one interface to another interface. When this process is getting executed, the new access network is marked as active and rest of the interfaces is marked as inactive. The communication path in the active interface is always transparent. Handover mechanisms in Heterogeneous Network steps (Figure 4.1) are
Step 1 : While HA performs Handover with MCoA first step of MR is to discover the whole MR’s in the entering interface network using TD with Neighbor Discovery (ND) and route advertisement, NINA and RRH protocols.

Step 2 : Next to send the NINA message to each entering interface of MR that advertises the subsequent flow of routes in the MR.

Step 3 : Then RRH is used to establish the path between the MR and HA and frequently update the record.

Step 4 : The next step is to obtain the neighbor links by sending the RtSolPr (proxy advertisement) to MNN.

Step 5 : When MR receives acknowledgement (PrRtAdv) from HA, MR then creates NCoA for registration.

Step 6 : In the inactive interface HM establish new binding when it connects to new network.

Step 7 : After current node and new access network is connected, a burrow is established between MR and HA.

Step 8 : While the handover operation is performed using flow binding it moves from one interface to another interface.

Step 9 : When this process is getting executed, the new access network between MR and AP1 is marked as active and rest of the interfaces are marked as inactive.

Step 10 : The handover process is performed using flow binding. Flow binding is updated and binding acknowledgement received when flow binding moves from one interface to another interface.

Step 11 : The New Access Network between MR and AP2 marked as active and remaining interfaces are inactive. The communication path in the active interface is always transparent.
Step 12: The communication path in the active interface is always transparent.

Figure 4.1 Handover mechanisms in Heterogeneous Network
4.3.2 Security in Predictive Handover

To establish the safety transmission of BU data from the challenger attacks like hacking, MIMT attacks and DoS attack, the security requirements, proprietorship of the HoA, and reachability of the CoA are estimated using asymmetric cryptography. The Elliptic Curve Cryptographic (ECC) and the Elliptic Curve Digital Signature Algorithm (ECDSA) are used to provide protection for the BU messages (Brow 2010; Shaikh & Deotale 2015).

The Elliptic Curve Cryptography (ECC) is a public key cryptography method in which each and every user has public, private keys and set of operations relevant to those keys. The major benefit of ECC is that it uses key with smaller size for using encryption and decryption. It is more efficient, consumes less memory space, bandwidth, less power and faster. The sender can encrypt the messages with help of receiver’s public key and followed by signed encrypted message using its private key. Subsequently the received message is decrypted using its own private key and find out with help of sender’s public key.

4.3.2.1 Applying Elliptic Curve Digital Signature Algorithm in EFMNEMO+

Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematical illustration for the elliptic curve analogue of the DSA. This main feature is secure and faster distribution of information after authenticating the users in environment where amount of storage utilized is less within a lesser response time. VANET uses Asymmetric ECDSA key pair for user authentication purpose and to verify the signatures. An asymmetric key pair of the public and private key is used in ECDSA. The public key is a
random multiple of the base point and the private key is the integer used to produce the random multiple. User validation is done in two steps. The first one is public key validations which avoids the change of attacks rised from use of invalid public keys and find the transmission errors. The second is invoking the user authentication by validating private key. This method provides high level of reliability of transmission and security. The ECDSA is used to reduce the scope of attacks from malicious users. Elliptic Curve Digital Signature algorithm contains three phases

- Key generation
- Signature generation
- Signature verification

A setup phase has to be processed before the key generation phase to produce the domain parameters. Domain parameters for an elliptic curve describe an elliptic curve $Z$ defined over a finite field $F_s$, a base point $p \in Z (F_s)$ (generator) with order $n$. The parameters should be chosen carefully so that ECDLP is resistant to all known attacks. The elliptic curve is chosen by choosing $(x, y) \in (1, s)$ and substituting in equation. So the domain parameters can be defined as $s, Z (x, y), p, \text{and } n$.

CN waits for false binding; MN is verifies the reachability of MR and address proprietorship. NEMO+ depends on MR Private Key and hash function is calculated for authenticating the authority of MR with MR private key and valid subnet prefix, the proprietorship of MR Internet Protocol address is verified by CN.

Second reachability of MR is verified by PKBU. In this process, MA sends hash value of the MR HOA, MR public key and request for the CN
public key to the CN through Home Agent (HA). When MR gets the CN public key, messages are directly send to CN. With CN public key, MR encrypt the MR CoA and HOA in the message. While message reaches CN, it uses the MR public key to check the signature and then MN CoA and HOA is gained after decrypting the message. Next step is to make CN compare the hash value of HOA with hash value of received message from MR. Through verifying and validating the MR HOA and CoA output is positive then the CN permits MR to register with CoA.

The interchanging of messages within the nodes in the PKBU protocol suggests three types of stages. The first stage is to establish the partnership of the MR’s IP address which associates in one of three steps. The second stage is the reachability of MR is justified. The last stage is validation process which contains four steps. The validation process executing stage CN has to ensure partnership of MR and reachability of HoA and CoA.

**Stage1: Partnership of the MR’s IP**

MR produces its private, public key and interface ID through the following three steps (Figure 4.2).

- **Creating private key**

  The MR’ private key is produced by User Identity Number (UIN) is an integer value. A hash function with arbitrary produced integer value of an UIN is computed to generate MR’s private key is given below,

  \[ NT_{RK} = Hash(UIN) \ast n \] (4.1)
Where, \( NT_{RK} \) is MR private key and \( n \) is a random integer value ranges 1 to \( m-1 \).

- **Creating public key**

  During this processing stage, MR generates its own public key. By using ECC, the public key of MR is produced with the MR’s private key. Deal with the equation 4.2

  \[
  q_2 = r_3 + mr + n \quad (4.2)
  \]

  where \((r,q)\) are points on the curve and \( n \) values produced for curve. The bounds of ECC are \( C = \{ m, n, X, y \} \) where \( m, n \) are values of the elliptic curve, \( X \) is base point of elliptic curve and \( y \) is the order of curves. MR’s public key \( (MR_{st}) \) is produced using the MR’s private key \( (MR_{RK}) \) and then MR’s public key \( (MR_{st}) \) is \( MR_{RK} \cdot X \) where \( X \) is a point P.

  Consequently \( MR_{st} \) is point of the curve that is produced by private key. To verify the partnership of the MR’s IP address has both public and private keys.

  \[
  MR_{st} = MR_{RK} \cdot X \quad (4.3)
  \]

- **Creating Interface ID**

  This step is followed by the creation of interface ID as 128 bit address, 64 bit address given by prefix and 64 bit for interface identifier that are obtained from hash value of MR’s private key. This process generates secure bind between MR’s interface ID and its own private key without associate PKI.
Stage 2: Reachability of the MR to CN

It is reached by sending the CoA to CN over HA by way of IP moment. Every time MR is ingress in new network. It should register with new CoA and the process of HA is finished before MR utilizes new CoA. The following steps are done to make sure the reachability of MR to CN.

Step 1: MR forward message to CN. MR forwards the specifications for routing optimization to CN through HA. In the prior (set up) burrow forwards hash value of MR’s HoA, public key of MR and call for the public key of CN through HA to CN.

Step 2: CN forwards messages to MR so that the MR gets the CN’s public key by using HA. The Hash values of MR’s HoA and MR’s public key are saved in CN.
Step 3: MR message is encrypted by applying CN’s public key. The MR encrypts the MR’s CoA and HoA and the above cipher text are signed using MR’s private key.

- Stage 3: Validation Process

The validation process stage helps to validate the progress of the requirements for security, partnership and reachability of the MN’s IP addresses. CN authorize the MR signature by applying the MR’s private key. Verification of CN is done by decrypting with the CN’s private key to benefit MR’s CoA and HoA. The CN message assures the HoA by measuring the hash value of decrypted HoA and the results are matched with the hash value of HoA which are sent through MR.

If the results are negative, the time message will have to be banned and if the process result is positive, it approves the partnership of MR and when CoA is known, the next step is to make MR reachable to CN. This will forward the Binding Acknowledgement (BA) message to MR. The overall flowchart and pseudocode of proposed SEFMNEMO+ are given in Figure 4.3 and 4.4.
Figure 4.3 Flow Diagram
Input: Handovers, Hacking the FBU message

Output: Produce seamless connectivity with reduce delay and loss in packet, secures over the transmission of FBU message.

Begin:

For each MR in the network
Discover and connects MRs using tree discovery.
Ensure the routes of connected MR sending the NINA message.
If NINA present then
    Trace the path of destined MNN
Else
    Record the actual CoA of MR.
End If
End for

//** HANDOVER PROCESS**

For each time handover
If FBBack received before trigger of layer 2 then
    MR→RtSolPr to PAR
Until (MR→PrRtAdv)
//** Proprietorship of the MR’s IP**

\[
MR_{PR} = \text{Hash}(\text{UI}) \times m
\]
\[
MR_{PU} = MR_{PR} \cdot P
\]

UID←128 bit address

//**Reachability of the MR to CN**

For MR to CN then
MR(CoA)→Hash (MR (HoA)), MNPUK, ReqCNPUK→HA
HA→Hash (MN (HoA)), MNPUK, ReqCNPUK→CN
    CNA -> CN_{PUK} -> MN

MN (CoA)→SignMR(PRK) (EncryptCN(PUK)) ( MN(CoA), MN (HoA))→CN
If (MNN receive BU) then
Advance registration ←NCoA.
End If

BCE[] ←MR’s HoA
**BUFFERING THE PACKETS TO NAR**

For \( N=0 \) to \( n-1 \)

\[ \text{NARbuf}[] \leftarrow \text{packets from HA} \]

End if

**SEND THE BUFFERED PACKETS TO MNN**

For \( \forall \) packets in \( \text{NARbuf}[] \)

\[ \text{NARbuf}[] \rightarrow \text{packets to MNN}. \]

End for

Else

/** Proprietorship of the MR's IP **/

\[ \text{MR}_{FR} = \text{Hash} (\text{UI}) \ast m \]

\[ \text{MR}_{PU} = \text{MR}_{FR} \ast P \]

User interface ID \( \rightarrow \) 128 bit address

/** Reachability of the MR to CN **/

For MR to CN

\[ \text{MR}(\text{CoA}) \rightarrow \text{Hash} (\text{MR (HoA)}), \text{MNPUK}, \text{ReqCNPUK} \rightarrow \text{HA} \]

\[ \text{HA} \rightarrow \text{Hash} (\text{MN (HoA)}), \text{MNPUK}, \text{ReqCNPUK} \rightarrow \text{CN} \]

\[ \text{CN} \rightarrow \text{CN}_{PUK} \rightarrow \text{HA} \]

\[ \text{HA} \rightarrow \text{CN}_{PUK} \rightarrow \text{MN} \]

\[ \text{MN} (\text{CoA}) \rightarrow \text{SignMR(PRK)} (\text{EncryptCN} (\text{PUK}) (\text{MN(CoA)}, \text{MN} (\text{HoA}))) \rightarrow \text{CN} \]

If (\( \text{MNN receive BU} \)) then

Sends UNA message to PAR

Until (NAR receives ACK)

** exchanhing HI and HACK message **

NAR \( \rightarrow \) HI to PAR

PAR \( \rightarrow \) HACK to NAR

End

Figure 4.4 Pseudocode of SEFMNEMO+
4.4 EXPERIMENTAL ANALYSIS

This proposed methodology is used to analyze the security, handover efficiency and its performance. NS-2 network simulation tool is implemented in this proposed methodology. In this simulation work, the network contains of 20 handover mechanisms and 100 mobiles nodes. This work shows an efficient result of proposed protocol when related with existing system. The packet loss, average delay, control overhead and average throughputs are measured using SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ in this work. These outcomes are briefly explained below.

Figure 4.5 Packet Loss Ratio Vs Handoff_Nodes
The packet loss ratio that occurred during handover for existing and proposed methods is illustrated in the Figure 4.5. The packet loss ratio of SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ achieved are 5.5 %, 8 %, 11.5 % and 14.5 % for 5 number of handoff nodes, 9.5 %, 12.25 %, 21.8% and 24.5 % for 10 number of handoff nodes, 13 %, 19.5 %, 28 % and 30.0 % for 15 number of handoff nodes and 20.5 %, 23.5 %, 32.5 % and 35.5 % for 20 number of handoff nodes during handover. It is observed that proposed SEFMNEMO+ method provides less packet loss ratio when compared to other methods. The packet loss is represented by percentage (%).

![Figure 4.6 Packet Loss Ratio Vs Node_Speed](image)

Figure 4.6 Packet Loss Ratio Vs Node_Speed

The Figure 4.6 illustrates that packet loss ratio for existing and proposed methods with varying node’s speed. The packet loss ratio of SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ achieved are 3.8 %, 9 %, 9.75 % and 14.5 % for node’s speed of 5ms, 7.75 %, 12.5 %,
13.8% and 19.8% for node’s speed of 10ms, 13.25 %, 15.75 %, 18 % and 25 % for node’s speed of 15ms and 8.5 %, 22.75 %, 26.25 % and 30.5 % for varying node’s speed of 20ms. From the figure, it is analyzed that proposed SEFMNEMO+ method provides less packet loss ratio when compared to other methods. The packet loss is represented by percentage (%).

**Figure 4.7 Average Delay Vs Handoff_Nodes**

The average handover delay for existing and proposed methods during handover in the network is shown in Figure 4.7. During handover, SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ achieved an average handover delay of 1.5 ms, 3.8 ms, 5.8 ms and 7.75 ms for 5 number of handoff nodes, 7.75 ms, 9.5 ms, 11.8 ms and 14.8 ms for 10 number of handoff nodes, 13.8 ms, 19.6 ms, 22 ms and 25 ms for 15 number of handoff nodes and 19.25 ms, 24.8 ms, 28.25 and 29.25 ms for 20 number of handoff nodes. From the graph, it is inferred that the proposed SEFMNEMO+ method
provides less average delay when compared to other methods. The average delay is represented by milliseconds (ms).

![Figure 4.8 Average Delay Vs Node_Speed](image)

**Figure 4.8 Average Delay Vs Node_Speed**

The illustration of the average packet delay occurred during handover for existing and a proposed method with varying node’s speed in the network is mentioned in Figure 4.8. The average delay of SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ achieved are 1.5 ms, 3.8 ms, 5.8 ms and 7.5 ms for node’s speed of 5ms, 7.5 ms, 9.5 ms, 11.8 ms and 14.75 ms for node’s speed of 10ms, 11.8 ms, 19.5 ms, 22 ms and 25 ms for node’s speed of 15ms and 18.3 ms, 24.6 ms, 28.25 and 29.5 ms for node’s speed of 20ms. From the graph, it is found that the proposed SEFMNEMO+ method provides less average delay when compared to other methods. The average delay is represented by milliseconds (ms).
Figure 4.9 Overhead Vs Handoff_Nodes

The overhead that occurred for existing and proposed methods during handover in the network is illustrated in the Figure 4.9. During handover, the overhead obtained for SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ methods are 2.5, 4.5, 8.75 and 11.8 for 5 number of handoff nodes, 8.5, 8.75, 13.5 and 16.25 for 10 number of handoff nodes, 12.5, 14.25, 18.25 and 19.5 for 15 number of handoff nodes and 13.5, 17.5, 19.5 and 23.75 for 20 number of handoff nodes. From the graph, it is analyzed that proposed SEFMNEMO+ method provides less control overhead when compared to other methods.
The Figure 4.10 illustrates the overhead that occurred for existing and proposed methods with varying node’s speed in the network. The achieved values of overhead related to the proposed methods SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ are found to be 2.75 kbps, 4.75 kbps, 8.8 kbps and 11.8 kbps for node’s speed of 5ms, 8.5 kbps, 9.75 kbps, 13.5 kbps and 16.25 kbps for node’s speed of 10ms, 12.5 kbps, 14.25 kbps, 18.3 kbps and 19.5 kbps for node’s speed of 15 ms and 14.5 kbps, 17.5 kbps, 21.5 kbps and 23.5 kbps for node’s speed of 20ms respectively. From the graph, it is inferred that the proposed SEFMNEMO+ method provides less overhead when compared to other methods.
The throughput that occurred for existing and proposed methods during handover in the network is mentioned in the Figure 4.11. During handover, the throughput obtained for SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ are 14.5 kbps, 13 kbps, 9.75 kbps and 7.5 kbps for 5 number of handoff nodes, 17.5 kbps, 17.9 kbps, 11.8 kbps and 11.5 kbps for 10 number of handoff nodes, 25 kbps, 25.75 kbps, 12 kbps and 12 kbps for 15 number of handoff nodes, 29.5 kbps, 28.2 kbps, 15.5 kbps and 15.75 kbps for 20 number of handoff nodes. From the graph, it is analyzed that proposed SEFMNEMO+ method provides high throughput when compared to other methods. The throughput is represented by kilo bytes per seconds (kbps).
Figure 4.12 Throughput Vs Node Speed

The Figure 4.12 illustrates that throughput for existing and proposed methods with varying node’s speed in the network. The throughput of SEFMNEMO+, EFMNEMO+, EFNEMO+ and existing NEMO+ achieved are 14.5 kbps, 13 kbps, 9.8 kbps and 7.5 kbps for node’s speed of 5ms, 17.5 kbps, 17.8 kbps, 11.8 kbps and 10.7 kbps for node’s speed of 10ms, 23.2 kbps, 24.5 kbps, 12 kbps and 12 kbps for node’s speed of 15ms, 29.2 kbps, 27.2 kbps, 14.25 kbps and 15.25 kbps for node’s speed of 20ms. From the graph, it is analyzed that proposed SEFMNEMO+ method provides high throughput when compared to other methods. The throughput is represented by kilo bytes per seconds (kbps).
4.5 SUMMARY

Multihoming concept is used to establish Always Best Connected Network in a wireless environment under multi access situations. This chapter is focused on the new methodology called SEFMNEMO+ that improves the seamless connectivity and improve the security mechanism in multi-homing environment. Elliptic Curve Digital Signature Algorithm (ECDSA) is used to protect the BU messages. This proposed method is reduced packet loss, average delay, and overhead and increased throughput. This experimental result shows an efficient result of proposed protocol when compared with existing system. Due to lack of target selection of network, the performance of the handover is found to get degraded in a heterogeneous network. This problem can be overcome by optimizing SEFMNEMO+ by applying Fuzzy concept that determine the optimal selection of network for a handover which protect the continuity and the quality of service provided by network.