7005 Asn4 - Design

We use bytes for everything!

John Agapeyev; A00928238
Isaac Morneau; A00958405

Send ACK	10
Wait ACK Delay	10

Protocol Sizes

Cipher Length - plaintext len + 16 bytes
IV - 16 bytes FIXED SIZE
HMAC - 32 bytes FIXED SIZE

Delays

100ms - tentative

Packet Structure

External Packet Protocol:

Field	Length	Ciphertext	IV	HMAC
Size (Bytes) **Total: 66 to 1074**	2	16 to 1024	16	32

Note: Plaintext will be capped at 1008 (1024-16)
Ciphertext will include protocol fields, see below.

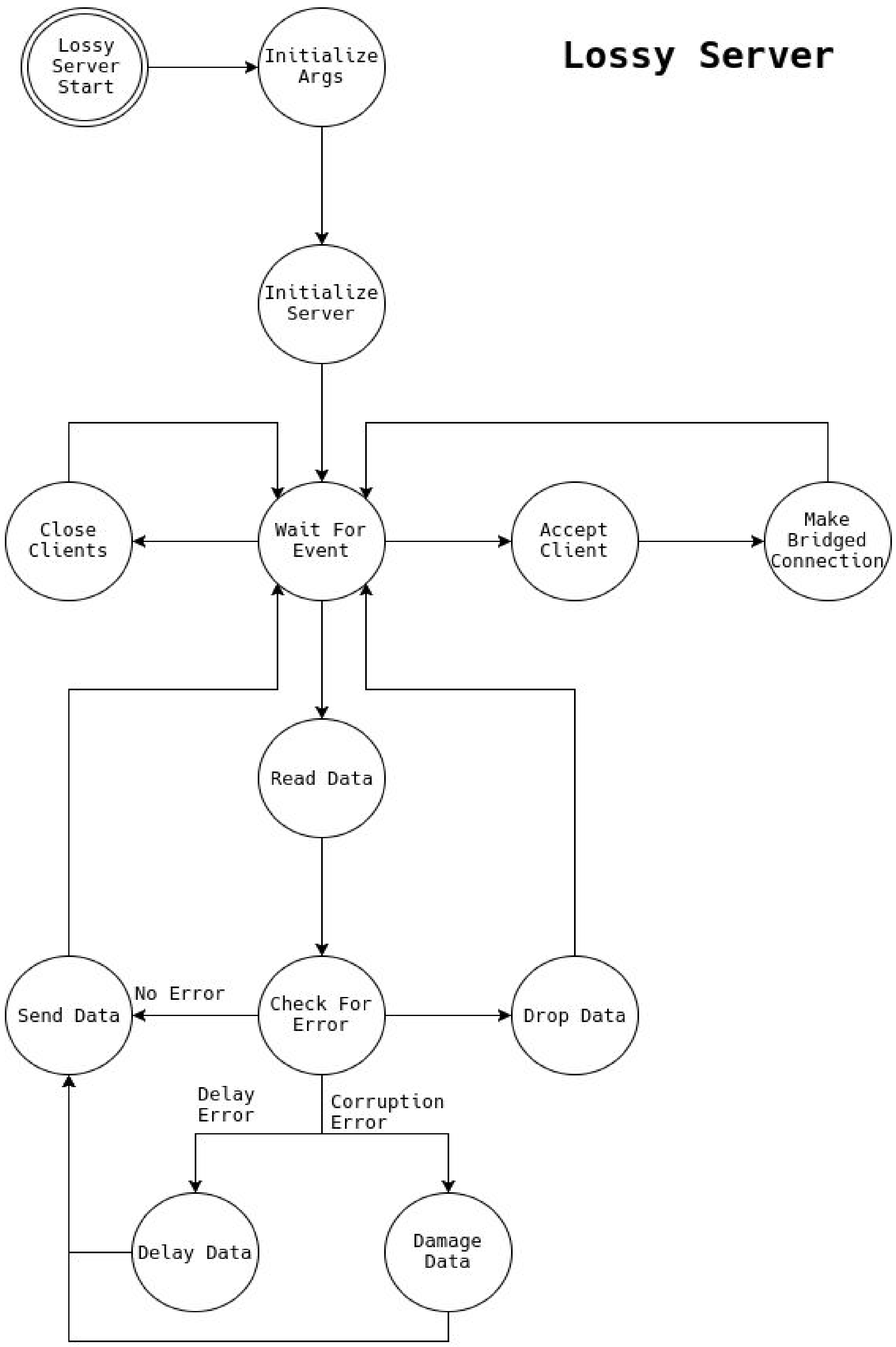
Ciphertext Protocol:

Field	Type(ACK, DATA)	SEQ	AC K	Window Size	Plaintext
Size (Bytes) **Total: 7 to 1008**	1	2	2	2	0 to 1001

Bonus Features

- Install script
- Cmake
- Epoll
- Pthreads
- Encryption
- Multi Language
- Full Duplex
- Signals

Lossy Server FSM



Pseudocode Lossy Server

Lossy Server Start

```
Goto Initialize Args
```

Initialize Args

```
Parse the selected error type
Parse the selected error rate
Parse the connection forwarding
Goto Initialize server
```

Initialize server

```
Make sockets
Bind sockets
Initialize epoll
Start listening
Goto Wait For Event
```

Wait for event

```
If the incoming event is a closed fd
    Goto Close Clients
If the incoming event is a new connection
    Goto Accept Client
Otherwise the data is a packet
    Goto Read Data
```

Close Clients

```
Close the resources used by the connection
Close the related bridged connection
Close the resources of the bridged connection
Goto Wait for event
```

Accept Client

```
Accept the incoming connection
Goto Make Bridged Connection
```

Make Bridged Connection

Create bridged connection
Link two connections
Goto **Wait for event**

Read Data

Read in a packet into the buffer
Goto **Check for error**

Check for error

```
If there is no error to inflict
    Goto Send data
If there is a drop error
    Goto Drop data
If there is a delay error
    Goto Delay data
If there is a corruption error
    Goto Damage data
```

Send data

Send buffered packet to bridged connection
Goto **Wait for event**

Drop data

Ignore the packet
Goto **Wait for event**

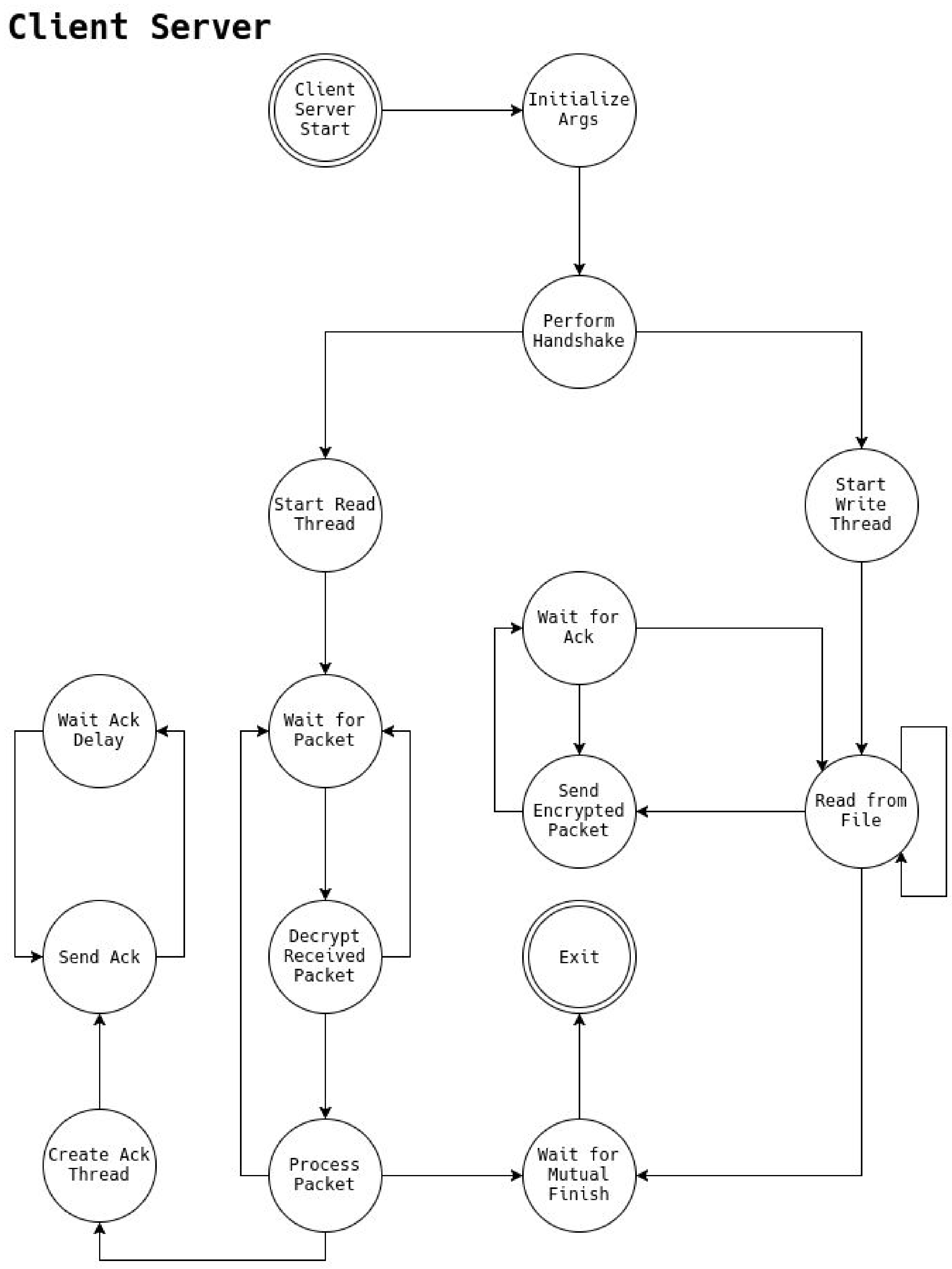
Delay data

Wait for the selected time out
Goto **Send data**

Damage data

XOR the bits to the selected BER
Goto **Send data**

Client Server FSM



Pseudocode Client Server

Client Server Start

```
Goto Initialize Args
```

Initialize Args

```
Parse mode for client or server
If mode is server
    Listen for connections
If mode is client
    Connect to server
Goto Perform Handshake
```

Perform Handshake

```
Send both server keys to client
Send both client keys to server
Generate shared secret from keys
Start thread goto Start Read Thread
Start thread goto Start Write Thread
```

Start Write Thread

```
Open file to send
Goto Read from File
```

Read from File

```
Read data from the file into buffer
Goto Send Encrypted Packet
```

Send Encrypted Packet

```
Encrypts the data
Sends the data
Goto Wait for ACK
```

Wait for ACK

```
Initialize timeout
If timeout occurs
    Goto Send Encrypted Packet
```

If ACK is received
    Goto **Read from File**

Wait for Mutual Finish

Spin lock on waiting for the other side to send fin packet

Start Read Thread

Opens file for writing
Goto **Wait for packet**

Wait for Packet

Read packet into buffer
Goto **Decrypt Received Packet**

Decrypt Received Packet

Check HMAC if failed

    Goto **Wait for Packet**
Decrypt Data
Goto **Process packet**

Process Packet

Check if packet is a duplicate
    Goto **Wait for Packet**
Write data to file
Start thread goto **Create ACK Thread**
Goto **Wait for packet**

Create ACK thread

Initialize time outs
Goto **Send ACK**

Send ACK

Send ACK with last received sequence
Goto **Wait for ACK Delay**

Wait ACK Delay

Wait for timeout

Goto **Send ACK**