ECS 132 Fall 2020, Project

December 1, 2020

Your name: Nicholas Treynor

Partner's name: James Lemkin

Any other collaborator(s):

Instructions

1. Please refer to "ECS_132_Project.pdf" for details.
2. You may in no circumstances upload your project to private tutoring websites such as CourseHero or Chegg. Remember all material related to this course is a property of the University of California and posting them is a violation of the copyright laws.
3. If you refer to a source (either a book or the internet), you must cite it.
4. You may work in groups of size of at most 2. If you collaborate with others, you must list their names.
5. Write your answers in R Markdown and submit the knitted pdf on Gradescope; for due date and other details see the Homework Policy and Schedule.

3 Design

3.1

Alice and Bob decide to use the following modulation scheme to map the bits to the inter-packet delay. A delay of 0.25 is used to encode a bit 0 and delay of 0.75 is used to encode a bit 1. Write a short R code that will generate the modified packet stream that contains the secret message.

charToRaw(x) - converts characters to hexadecimal value rawToBits(x) - converts hexadecimal value to bit values. The bits are in reverse order per decimal value, so the letter t corresponds to 74 in hexadecimal -> 01110100 in reality, but will return as 00101110 when using the function.

Answer

We want to output "this is a secret message". To do so, we need to convert the message into binary, and then send along the individual bits that make up the binary using the encoding delays.

We need to loop over the generated strings carefully, stepping 16 forward then looping backwards over 8 integers.

```
#  your R code here
message = "this is a secret message"
rawMessage = charToRaw(message)
bits = rawToBits(rawMessage)

bitLength = (nchar(message) * 8)
sentPacketsTime = numeric(bitLength + 1)
sentPacketsStream = numeric(bitLength)
sentPacketsDelays = numeric(bitLength)
currTime = 0
index = 2
for (i in 1:nchar(message)) {
  for (x in 0:7) {
    if (bits[(i*8) - x] == 00){
      sentPacketsTime[index] = currTime + 0.25
      currTime = currTime + 0.25
      sentPacketsStream[index-1] = 0
      sentPacketsDelays[index-1] = 0.25
    } else {
      sentPacketsTime[index] = currTime + 0.75
      currTime = currTime + 0.75
      sentPacketsStream[index-1] = 1
      sentPacketsDelays[index-1] = 0.75
    }
    index = index + 1
  }
}

print(sentPacketsStream)
```

```
##   [1] 0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 1 1 0 0 1 0 0
##  [38] 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 0
##  [75] 1 0 0 0 0 0 0 0 1 1 1 0 0 1 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0 1 1 0 1 1 1 0 0 1
## [112] 0 0 1 1 0 0 1 0 1 0 1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 1 1 0 1 0 1 1 0
## [149] 0 1 0 1 0 1 1 1 0 0 1 1 0 1 1 1 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 0 1 1 1 0
## [186] 1 1 0 0 1 0 1
```

```
print(sentPacketsDelays)
```

```
##   [1] 0.25 0.75 0.75 0.75 0.25 0.75 0.25 0.25 0.25 0.75 0.75 0.25 0.75 0.25 0.25
##  [16] 0.25 0.25 0.75 0.75 0.25 0.75 0.25 0.25 0.75 0.25 0.75 0.75 0.75 0.25 0.25
##  [31] 0.75 0.75 0.25 0.25 0.75 0.25 0.25 0.25 0.25 0.25 0.25 0.75 0.75 0.25 0.75
##  [46] 0.25 0.25 0.75 0.25 0.75 0.75 0.75 0.25 0.25 0.75 0.75 0.25 0.25 0.75 0.25
##  [61] 0.25 0.25 0.25 0.25 0.25 0.75 0.75 0.25 0.25 0.25 0.25 0.75 0.25 0.25 0.75
##  [76] 0.25 0.25 0.25 0.25 0.25 0.25 0.75 0.75 0.75 0.25 0.25 0.75 0.75 0.25 0.75
##  [91] 0.75 0.25 0.25 0.75 0.25 0.75 0.25 0.75 0.75 0.25 0.25 0.25 0.75 0.75 0.25
## [106] 0.75 0.75 0.75 0.25 0.25 0.75 0.25 0.25 0.75 0.75 0.25 0.25 0.75 0.25 0.75
## [121] 0.25 0.75 0.75 0.75 0.25 0.75 0.25 0.25 0.25 0.25 0.75 0.25 0.25 0.25 0.25
## [136] 0.25 0.25 0.75 0.75 0.25 0.75 0.75 0.25 0.75 0.25 0.75 0.75 0.25 0.25 0.75
## [151] 0.25 0.75 0.25 0.75 0.75 0.75 0.25 0.25 0.75 0.75 0.25 0.75 0.75 0.75 0.25
## [166] 0.25 0.75 0.75 0.25 0.75 0.75 0.25 0.25 0.25 0.25 0.75 0.25 0.75 0.75 0.25
## [181] 0.25 0.75 0.75 0.75 0.25 0.75 0.75 0.25 0.25 0.75 0.25 0.75
```

```
print(sentPacketsTime)
```

```
##   [1]  0.00  0.25  1.00  1.75  2.50  2.75  3.50  3.75  4.00  4.25  5.00  5.75
##  [13]  6.00  6.75  7.00  7.25  7.50  7.75  8.50  9.25  9.50 10.25 10.50 10.75
##  [25] 11.50 11.75 12.50 13.25 14.00 14.25 14.50 15.25 16.00 16.25 16.50 17.25
##  [37] 17.50 17.75 18.00 18.25 18.50 18.75 19.50 20.25 20.50 21.25 21.50 21.75
##  [49] 22.50 22.75 23.50 24.25 25.00 25.25 25.50 26.25 27.00 27.25 27.50 28.25
##  [61] 28.50 28.75 29.00 29.25 29.50 29.75 30.50 31.25 31.50 31.75 32.00 32.25
##  [73] 33.00 33.25 33.50 34.25 34.50 34.75 35.00 35.25 35.50 35.75 36.50 37.25
##  [85] 38.00 38.25 38.50 39.25 40.00 40.25 41.00 41.75 42.00 42.25 43.00 43.25
##  [97] 44.00 44.25 45.00 45.75 46.00 46.25 46.50 47.25 48.00 48.25 49.00 49.75
## [109] 50.50 50.75 51.00 51.75 52.00 52.25 53.00 53.75 54.00 54.25 55.00 55.25
## [121] 56.00 56.25 57.00 57.75 58.50 58.75 59.50 59.75 60.00 60.25 60.50 61.25
## [133] 61.50 61.75 62.00 62.25 62.50 62.75 63.50 64.25 64.50 65.25 66.00 66.25
## [145] 67.00 67.25 68.00 68.75 69.00 69.25 70.00 70.25 71.00 71.25 72.00 72.75
## [157] 73.50 73.75 74.00 74.75 75.50 75.75 76.50 77.25 78.00 78.25 78.50 79.25
## [169] 80.00 80.25 81.00 81.75 82.00 82.25 82.50 82.75 83.50 83.75 84.50 85.25
## [181] 85.50 85.75 86.50 87.25 88.00 88.25 89.00 89.75 90.00 90.25 91.00 91.25
## [193] 92.00
```

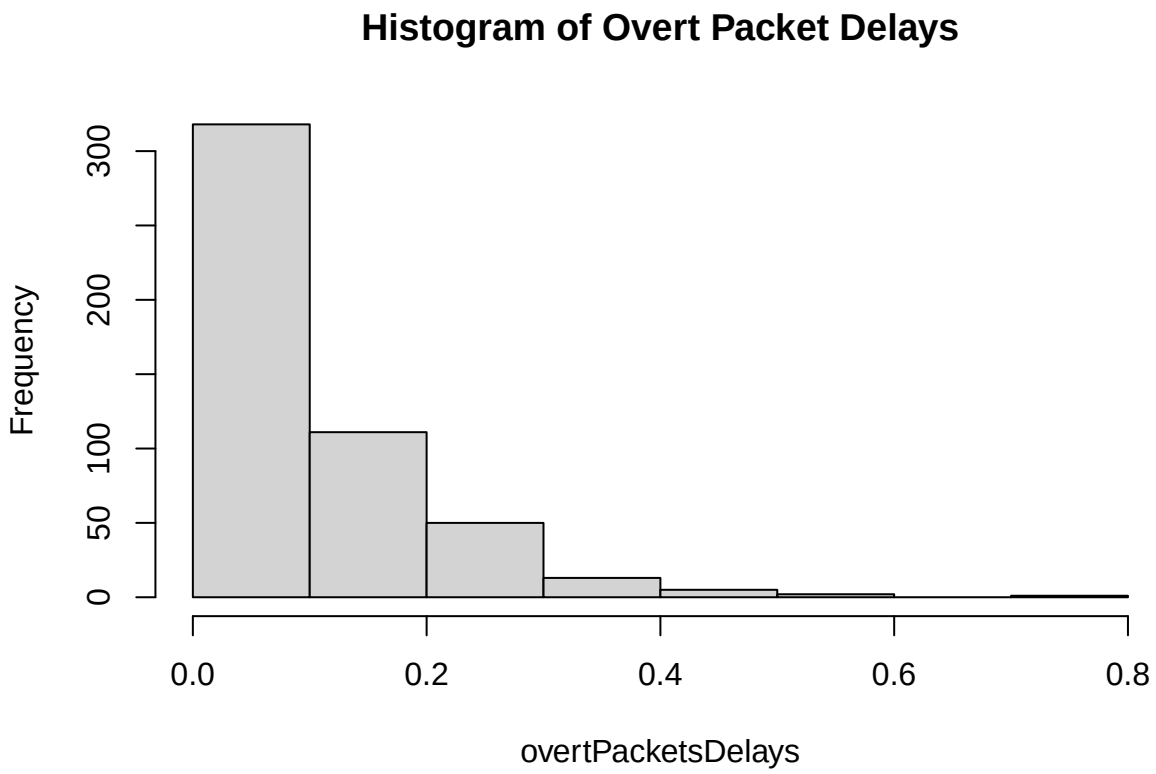
3.2

Plot the histogram of the inter-packet delays of the overt packet stream. Plot the histogram of the covert packet stream. Will Eve be suspicious?

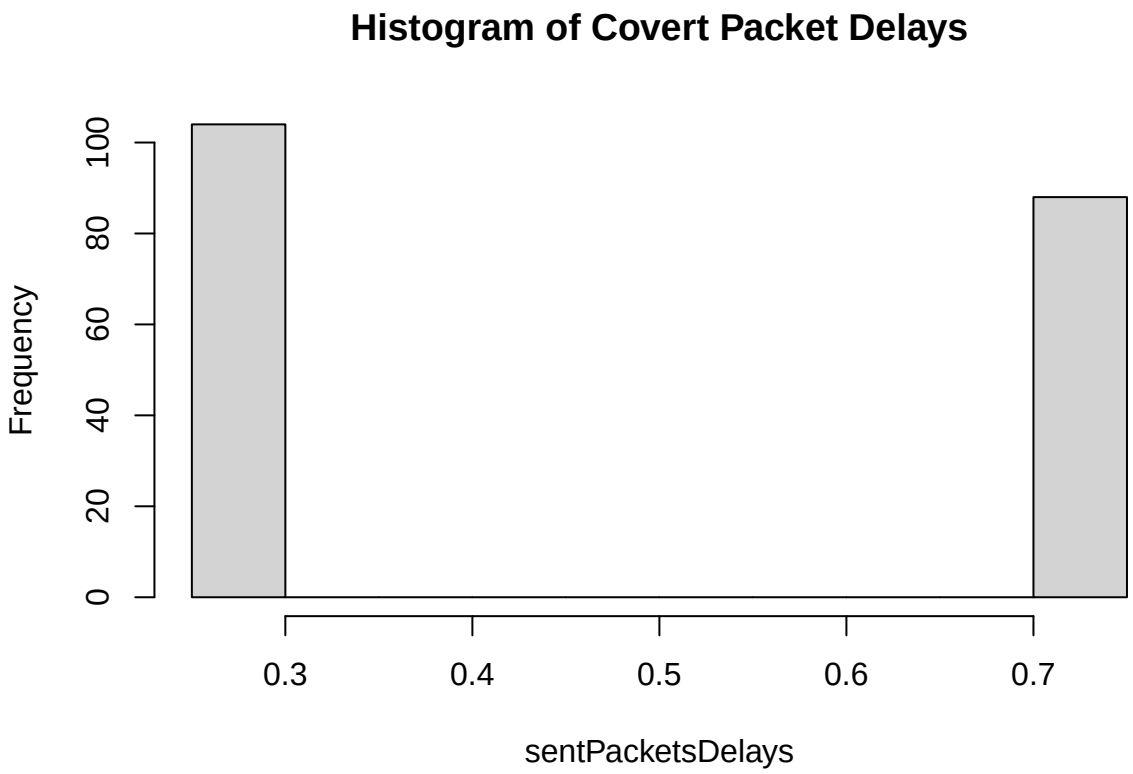
Answer

```
#  your R code here
data <- read.csv("Traffic_data_orig.csv", header=TRUE)
overtPacketStream = data[,2]
x = length(overtPacketStream)
overtPacketsDelays = numeric(x-1)
currTime = 0
index = 2
for (i in 2:x-1){
  overtPacketsDelays[i-1] = overtPacketStream[i]-overtPacketStream[i-1]
}

hist(overtPacketsDelays, main = "Histogram of Overt Packet Delays")
```




```
hist(sentPacketsDelays, main = "Histogram of Covert Packet Delays")
```



There is a very clear difference in the two histograms, indicating that some sort of unusual data transmission is occurring. Eve would be suspicious if she were monitoring our packet delays.

3.3

Alice and Bob decide to use the following modulation scheme. Let m, min, and max denote the median, min, and max of the inter-packet delay of the overt packet stream. If Alice needs to send a 0 she randomly generates a delay between min and m. If she want to send a 1 she randomly generates a delay between m and max. First, compute m, min, and max. Next, modify the code in Question 1, to generate the packet stream that contains the secret message.

Answer

```
#  your R code here
med = median(overtPacketsDelays)
min = min(overtPacketsDelays)
max = max(overtPacketsDelays)
mean = mean(overtPacketsDelays)

message = "this is a secret message"
rawMessage = charToRaw(message)
bits = rawToBits(rawMessage)

bitLength = (nchar(message) * 8)
```

```
sentPacketsTime = numeric(bitLength + 1)
sentPacketsStream = numeric(bitLength)
sentPacketsDelays = numeric(bitLength)
currTime = 0
index = 2
for (i in 1:nchar(message)) {
  for (x in 0:7) {
    if (bits[(i*8) - x] == 00){
      delay = rexp(1, 1/mean)
      while (delay > med || delay < min) {
        delay = rexp(1, 1/mean)
      }
      sentPacketsTime[index] = currTime + delay
      currTime = currTime + delay
      sentPacketsStream[index-1] = 0
      sentPacketsDelays[index-1] = delay
    } else {
      delay = rexp(1, 1/mean)
      while (delay <= med || delay > max) {
        delay = rexp(1, 1/mean)
      }
      sentPacketsTime[index] = currTime + delay
      currTime = currTime + delay
      sentPacketsStream[index-1] = 1
      sentPacketsDelays[index-1] = delay
    }
    index = index + 1
  }
}
```

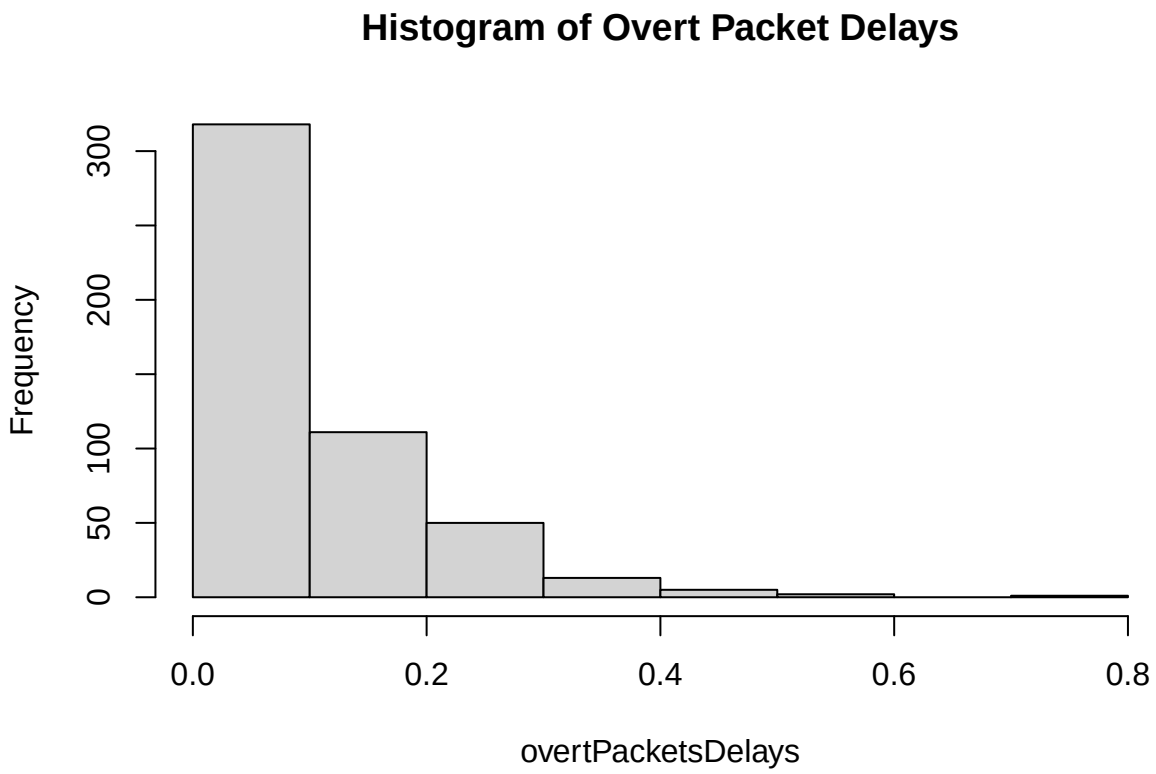
3.4

Plot the histogram of the inter-packet delays of the overt packet stream and that of the new covert packet stream. Do you think Eve will be suspicious?

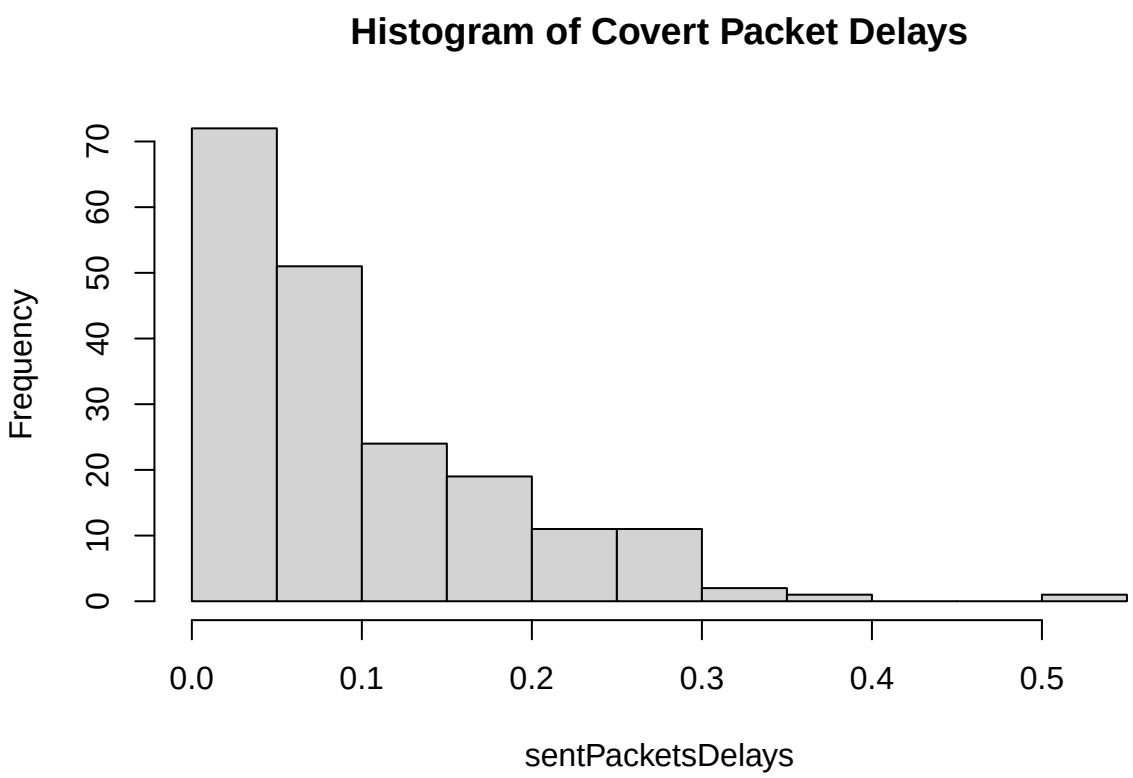
Answer

```
#  your R code here
data <- read.csv("Traffic_data_orig.csv", header=TRUE)
overtPacketStream = data[,2]
x = length(overtPacketStream)
overtPacketsDelays = numeric(x-1)
currTime = 0
index = 2
for (i in 2:x-1){
  overtPacketsDelays[i-1] = overtPacketStream[i]-overtPacketStream[i-1]
}

hist(overtPacketsDelays, main = "Histogram of Overt Packet Delays", breaks = 8)
```




```
hist(sentPacketsDelays, main = "Histogram of Covert Packet Delays", breaks = 8)
```



Eve will most likely not be suspicious because the distributions of the overt and covert packet delays are nearly indistinguishable from one another. The overt distribution looks like an exponential distribution so we sampled an exponential distribution with the same rate parameter as the overt distribution and bounded it in order to generate our delays.

3.5

Answer the following questions briefly (in 1 or 2 sentences)

1. How can you improve upon the method in Question 3?

   Answer: If we had access to more data we could potentially compute an even more precise rate parameter. Potentially another way we could approach this problem is by taking samples from the overt distribution and adding some noise to it. With this approach we wouldn't need to make assumptions about the underlying distribution.

2. We assumed the Alice will buffer up the packets and we mentioned that it was unrealistic. Why?

   Answer: In the case where we're using Skype and transmitting data, altering the delays of packets by buffering up a large number of them before sending them out would prevent the call from behaving normally – it may cause problems with the application or rouse suspicion if someone is watching. As a result, it could be problematic.

3. We have assumed that the network does not alter the inter-packet delays. What would be the problem if it did? Can you suggest methods to mitigate the effect of the changes of the inter-packet delay (noise)?

Answer: The problem could be that the timing delays could flip a 0 bit to a 1. There are multiple methods that we could use such as using a parity bit, re-sending the message multiple times, or increasing the odds of a correct transmission by moving the min and max thresholds for emitting a 0 or 1 away from the median.

4 Implementation

4.1

For buffer size $B = 20$ we want to find out the probability of overflow and underflow, when the IPD follows the Exponential with $\lambda = 1$ pkts/sec and $i = 2, 6, 10, 14, 18$. Use message size $m = 16, 32$ bits. Tabulate the results. Remember that to determine the probability you need to run multiple (say 500) experiments for each parameter, i.e., for $B = 20, m = 16, i = 2$ run 500 experiments and determine the probability of overflow and underflow. Similarly for other values of i and m.

Answer

```
#  your R simulation code here

ms = c(16, 32)
t = 500
B = 20
i = c(2, 6, 10, 14, 18)
for (m in ms) {
  OverflowProbability = numeric(5)
  UnderflowProbability = numeric(5)
  SuccessProbability = numeric(5)
  index = 0
  for (is in i) {
    index = index + 1
    overflows = numeric(t)
    underflows = numeric(t)
    for (x in 1:t) {
      message = sample(c(0, 1), size = m, replace = TRUE)
      CB = is

      packet_gen_delays = rexp(m, rate = 1)
      packet_send_delays = numeric(m)
      for (bit_i in 1:length(message)) {
        if (message[bit_i] == 0) {
          delay = rexp(1, 1)
          #while (delay > med || delay < min) {
          while (delay > 1 || delay < 0) {
            #print(delay)
            delay = rexp(1, 1)
          }
          packet_send_delays[bit_i] = delay
        } else {
          delay = rexp(1, 1)
          #while (delay <= med || delay > max) {
```

```
      while (delay <= 1) {
        #print(delay)
        delay = rexp(1, 1)
      }
      packet_send_delays[bit_i] = delay
    }
  }

  gen_i = is + 1
  t_next_gen = packet_gen_delays[gen_i]
  send_i = 1
  t_next_send = packet_send_delays[send_i]

  outcome = "success"

  while (gen_i < m) {
    if (t_next_gen < t_next_send) {
      # If  a packet will be added to the buffer before the next packet is sent
      t_next_send = t_next_send - t_next_gen

      gen_i = gen_i + 1
      t_next_gen = packet_gen_delays[gen_i]
      CB = CB + 1

      if (CB > B) {
        outcome = "overflow"
        break
      }
    } else if (t_next_send < t_next_gen) {
      # If we send the next packet before we generate the next packet
      t_next_gen = t_next_gen - t_next_send

      send_i = send_i + 1
      t_next_send = packet_send_delays[send_i]
      CB = CB - 1

      if (CB < 0) {
        outcome = "underflow"
        break
      }
    } else {
      # If we send a packet as we generate it
      gen_i = gen_i + 1
      t_next_gen = packet_gen_delays[gen_i]
      send_i = send_i + 1
      t_next_send = packet_send_delays[send_i]
    }
  }

  if (outcome == "overflow") {
    overflows[x] = 1
    underflows[x] = 0
  } else if (outcome == "underflow") {
```

```
        overflows[x] = 0
        underflows[x] = 1
      } else {
        overflows[x] = 0
        underflows[x] = 0
      }
    }



    z = mean(underflows) + mean(overflows)

    OverflowProbability[index] = mean(overflows)
    UnderflowProbability[index] = mean(underflows)
    SuccessProbability[index] = 1 - z
  }

  print(paste("Exponential Distribution"))
  print(paste("Message Size: ", m))
  df = data.frame(i, OverflowProbability, UnderflowProbability, SuccessProbability)
  print(df)
  table(df)
}
```

```
## [1] "Exponential Distribution"
## [1] "Message Size:  16"
##    i OverflowProbability UnderflowProbability SuccessProbability
## 1  2                    0                0.368              0.632
## 2  6                    0                0.064              0.936
## 3 10                    0                0.002              0.998
## 4 14                    0                0.000              1.000
## 5 18                    0                0.000              1.000
## [1] "Exponential Distribution"
## [1] "Message Size:  32"
##    i OverflowProbability UnderflowProbability SuccessProbability
## 1  2                0.002                0.478              0.520
## 2  6                0.034                0.134              0.832
## 3 10                0.142                0.020              0.838
## 4 14                0.356                0.008              0.636
## 5 18                0.726                0.000              0.274
```

```
# tabulate results and compute the probabilities
```

4.2

For buffer size $B = 20$ we want to find out the probability of overflow and underflow, when the IPD follows the Uniform distribution in the range (0,1) and $i = 2, 6, 10, 14, 18$. Use message size $m = 16, 32$ bits. Tabulate the results. Remember that to determine the probability you need to run multiple (say 500) experiments for each parameter, i.e., for $B = 20, m = 16, i = 2$ run 500 experiments and determine the probability of overflow and underflow. Similarly for other values of i and m.

Answer

```
#  your R simulation code here

ms = c(16, 32)
t = 500
B = 20
i = c(2, 6, 10, 14, 18)
for (m in ms) {
  OverflowProbability = numeric(5)
  UnderflowProbability = numeric(5)
  SuccessProbability = numeric(5)
  index = 0
  for (is in i) {
    index = index + 1
    overflows = numeric(t)
    underflows = numeric(t)
    for (x in 1:t) {
      message = sample(c(0, 1), size = m, replace = TRUE)
      CB = is

      packet_gen_delays = runif(m, 0, 1)
      packet_send_delays = numeric(m)
      for (bit_i in 1:length(message)) {
        if (message[bit_i] == 0) {
          delay = runif(1, 0, 0.5)
          packet_send_delays[bit_i] = delay
        } else {
          delay = runif(1, 0.5, 1)
          packet_send_delays[bit_i] = delay
        }
      }

      gen_i = is + 1
      t_next_gen = packet_gen_delays[gen_i]
      send_i = 1
      t_next_send = packet_send_delays[send_i]

      outcome = "success"

      while (gen_i < m) {
        if (t_next_gen < t_next_send) {
          # If  a packet will be added to the buffer before the next packet is sent
          t_next_send = t_next_send - t_next_gen

          gen_i = gen_i + 1
          t_next_gen = packet_gen_delays[gen_i]
          CB = CB + 1

          if (CB > B) {
            outcome = "overflow"
            break
          }
```

```
        } else if (t_next_send < t_next_gen) {
          # If we send the next packet before we generate the next packet
          t_next_gen = t_next_gen - t_next_send

          send_i = send_i + 1
          t_next_send = packet_send_delays[send_i]
          CB = CB - 1

          if (CB < 0) {
            outcome = "underflow"
            break
          }
        } else {
          # If we send a packet as we generate it
          gen_i = gen_i + 1
          t_next_gen = packet_gen_delays[gen_i]
          send_i = send_i + 1
          t_next_send = packet_send_delays[send_i]
        }
      }

      if (outcome == "overflow") {
        overflows[x] = 1
        underflows[x] = 0
      } else if (outcome == "underflow") {
        overflows[x] = 0
        underflows[x] = 1
      } else {
        overflows[x] = 0
        underflows[x] = 0
      }
    }



    z = mean(underflows) + mean(overflows)

    OverflowProbability[index] = mean(overflows)
    UnderflowProbability[index] = mean(underflows)
    SuccessProbability[index] = 1 - z
  }
  print(paste("Uniform Distribution"))
  print(paste("Message Size: ", m))
  df = data.frame(i, OverflowProbability, UnderflowProbability, SuccessProbability)
  print(df)
  table(df)
}
```

```
## [1] "Uniform Distribution"
## [1] "Message Size:  16"
##    i OverflowProbability UnderflowProbability SuccessProbability
## 1  2                   0                0.426              0.574
## 2  6                   0                0.014              0.986
```

```
## 3 10                  0               0.000              1.000
## 4 14                  0               0.000              1.000
## 5 18                  0               0.000              1.000
## [1] "Uniform Distribution"
## [1] "Message Size:  32"
##    i OverflowProbability UnderflowProbability SuccessProbability
## 1  2               0.000                0.594              0.406
## 2  6               0.000                0.150              0.850
## 3 10               0.002                0.002              0.996
## 4 14               0.032                0.000              0.968
## 5 18               0.442                0.000              0.558
```

```
# tabulate results and compute the probabilities
```

4.3

Propose methods to deal with buffer overflow and underflow.

Answer

Sending shorter messages, using larger buffers, ensuring that the buffer is half filled with packets when transmission begins, and ensuring that packet delays are generated using the appropriate distribution all ensure that buffer overflow and underflow has a low probability of occurring.

In the event that a buffer overflow or underflow occurs, we believe the best way to handle it would be to send a message to the receiver that a buffer overflow or underflow has occurred. This could be done by spiking the delay of a packet to be longer than usual. If using a uniform distribution, you could set the packet delay to be longer than the maximum normal delay, indicating that the previous packet needs to be resent. If overflow occurs, a similar spiked message could be sent, and then the receiver could know to ignore the next 5 packet delays, as the sender clears out some of the packets from the overflowed buffer at a slightly higher than normal rate. To use this method with an exponential distribution, the sender and receiver would need to place a cap on the length of delays generated by the sender, with the understanding that any delay longer than the agreed upon max indicates a problem.

Both of these methods do contain a slight risk of anomalous behavior being detected by a savvy Eve, however. A better method perhaps would be to transmit the same message multiple times, in the hopes that at least one such message would arrive intact.