VANET Assignment-2

Indian Institute of Technology, Jodhpur

CSL7310: Vehicular Ad-hoc Network

Submitted By:

Umang Barbhaya (M20CS017)

MTech in Computer Science

Indian Institute of Technology, Jodhpur

Course Instructor:

Dr. Debasis Das

Assistant Professor

Indian Institute of Technology, Jodhpur

Figure 1 presents the meaning of communication in VANET. Analyse the figure and answer the following. Table 1 represents the execution time required to calculate the cryptographic functions and table 2 represents the priority, size of different types of messages. The channel capacity is 2Mbps.

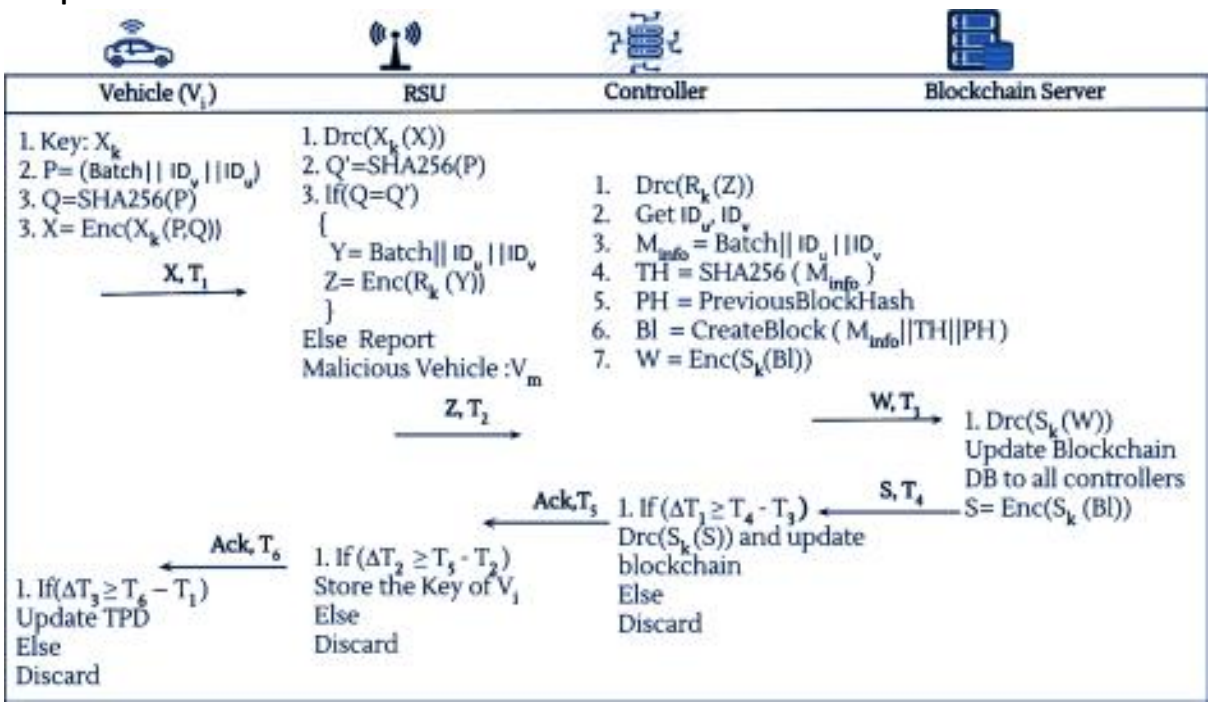

Figure1: Communication between different entities of VANET

Table1	
Cryptographic function	Execution Time (in milliseconds)
AES encryption (Enc(S_k(x))	1.534
AES encryption (Drc(S_k(x))	1.834
SHA256	0.0083
XOR	0.00012
Concatenation	0.00015

Table2		
Types of messages	Size (in bytes)	Priority
Accident M1	2 Byte	1
Traffic Jam M2	5 Byte	2
Bad Road M3	10 Byte	3
Construction site M4	18 Byte	4

Note: Except for all these messages, the size required to store a variable is 1 byte. The priority is high to low from top to bottom in the table.

Some Assumptions:

1. Size of SHA-256 hash digest = 1 byte
2. Size of any ID's = 1 byte
3. Size of any Timestamp = 1 byte
4. Size of ACK = 1 byte
5. Size of Key Xk = 1byte

1. **How much time it will take to propagate all these messages (i.e., from M1 to M4) including all the computation and communication cost?**
   Answer:
   Computation Cost:
   Number of concatenation: 8
   Number of Encryption: 4
   Number of Hashing: 3
   Number of Decryption: 4

   Concatenation Computation Cost: 8*0.00015 = 0.0012 ms
   Encryption Computation Cost: 4*1.534 = 6.136 ms
   Hashing Computation Cost: 3*0.0083 = 0.0249 ms
   Decryption Computation Cost: 4*1.834 = 7.336 ms

   Computation Cost = 13.4981 ms

   Communication Cost:

   - Cost for message M1 (M1 size = 2bytes)
     - From Vehicle to RSU
       Key(Xk) size = 1 byte … Assumption
       P size = M1 size + IDv size + IDu size = 2 + 1 + 1 = 4 byte
       Q size = SHA256(P) = 1 byte … Assumption
       Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 4 + 1 = 6 bytes
       Total size = Timestamp + X = 1+6 = 7 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 4 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 4 = 5 byte
  Total size = Timestamp + Y = 1+5 = 6 bytes

- From Controller to Blockchain Server
  Key(Sk) size = 1 byte … Assumption
  Minfo size = P size = 4 bytes
  TH size = SHA256(Minfo) = 1 byte … Assumption
  PH size = Previous Block Hash= 1 byte … Assumption
  BI size = Minfo + TH size + PH size = 4 + 1 + 1 = 6 byte
  Encryption Size (W) = Key(Sk) size + BI size = 1 + 6 = 7 bytes
  Total size = Timestamp + W = 1+7 = 8 bytes

- From Blockchain Server to Controller
  Encryption Size (S) = Encryption Size (W) = 7 bytes
  Total size = Timestamp + S = 1+7 = 8 bytes

- From Controller to RSU
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

- From RSU to Vehicle
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

Total Size for Message M1 = 7 + 6 + 8 + 8 + 2 + 2 = 33 bytes

Cost for message M2 (M2 size = 5 bytes)

- From Vehicle to RSU
  Key(Xk) size = 1 byte … Assumption
  P size = M2 size + IDv size + IDu size = 5 + 1 + 1 = 7 byte
  Q size = SHA256(P) = 1 byte … Assumption
  Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 7 + 1 = 9 bytes
  Total size = Timestamp + X = 1+9 = 10 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 7 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 7 = 8 byte
  Total size = Timestamp + Y = 1+8 = 9 bytes

- From Controller to Blockchain Server
  Key(Sk) size = 1 byte … Assumption
  Minfo size = P size = 7 bytes
  TH size = SHA256(Minfo) = 1 byte … Assumption
  PH size = Previous Block Hash= 1 byte … Assumption
  BI size = Minfo + TH size + PH size = 7 + 1 + 1 = 9 byte
  Encryption Size (W) = Key(Sk) size + BI size = 1 + 9 = 10 bytes
  Total size = Timestamp + W = 1+7 = 11 bytes

- From Blockchain Server to Controller
  Encryption Size (S) = Encryption Size (W) = 10 bytes
  Total size = Timestamp + S = 1+10 = 11 bytes

- From Controller to RSU
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

- From RSU to Vehicle
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

Total Size for Message M2 = 10 + 9 + 11 + 11 + 2 + 2 = 45 bytes

Cost for message M3 (M3 size = 10 byte)

- From Vehicle to RSU
  Key(Xk) size = 1 byte … Assumption
  P size = M3 size + IDv size + IDu size = 10 + 1 + 1 = 12 byte
  Q size = SHA256(P) = 1 byte … Assumption
  Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 12 + 1 = 14 bytes
  Total size = Timestamp + X = 1+14 = 15 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 12 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 12 = 13 byte
  Total size = Timestamp + Y = 1+13 = 14 bytes

- From Controller to Blockchain Server
  Key(Sk) size = 1 byte … Assumption
  Minfo size = P size = 12 bytes
  TH size = SHA256(Minfo) = 1 byte … Assumption
  PH size = Previous Block Hash= 1 byte … Assumption
  BI size = Minfo + TH size + PH size = 12 + 1 + 1 = 14 byte
  Encryption Size (W) = Key(Sk) size + BI size = 1 + 14 = 15 bytes
  Total size = Timestamp + W = 1+7 = 16 bytes

- From Blockchain Server to Controller
  Encryption Size (S) = Encryption Size (W) = 10 bytes
  Total size = Timestamp + S = 1+15 = 16 bytes

- From Controller to RSU
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

- From RSU to Vehicle
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

Total Size for Message M3 = 15 + 14 + 16 + 16 + 2 + 2 = 65 bytes

Cost for message M4 (M4 size = 18 byte)

- From Vehicle to RSU
  Key(Xk) size = 1 byte … Assumption

P size = M4 size + IDv size + IDu size = 18 + 1 + 1 = 20 byte
Q size = SHA256(P) = 1 byte … Assumption
Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 20 + 1 = 22 bytes
Total size = Timestamp + X = 1+22 = 13 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 20 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 20 = 21 byte
  Total size = Timestamp + Y = 1+21 = 22 bytes

- From Controller to Blockchain Server
  Key(Sk) size = 1 byte … Assumption
  Minfo size = P size = 20 bytes
  TH size = SHA256(Minfo) = 1 byte … Assumption
  PH size = Previous Block Hash= 1 byte … Assumption
  BI size = Minfo + TH size + PH size = 20 + 1 + 1 = 22 byte
  Encryption Size (W) = Key(Sk) size + BI size = 1 + 22 = 23 bytes
  Total size = Timestamp + W = 1+7 = 24 bytes

- From Blockchain Server to Controller
  Encryption Size (S) = Encryption Size (W) = 23 bytes
  Total size = Timestamp + S = 1+23 = 24 bytes

- From Controller to RSU
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte

- From RSU to Vehicle
  Total Size = Timestamp + ACK = 1 + 1 = 2 byte
  Total Size for Message M4 = 23 + 22 + 24 + 24 + 2 + 2 = 97 bytes

Total size for all messages 33+45+65+97 = 240 bytes
Bandwidth 2Mbps
1 Mbps = 125 Byte/ms
2 Mbps = 2*125=250 Byte/ms

Communication Cost = Total size/bandwidth=240/250=0.96 ms

Propagation Cost = Computation Cost + Communication Cost = 13.4981 + 0.96 = 14.4581ms

2. **What will be the storage requirement to store complete one transaction (including everything required to propagate the information in the network for each type of message?**
   Answer:
   As calculated above
   Storage cost of M1: 33 bytes
   Storage cost of M2: 45 bytes
   Storage cost of M3: 65 bytes
   Storage cost of M4: 97 bytes

3. **If an accident happened at the bad conditioned construction road**
   a. **How many messages are required to be communicated and what time it will take to transmit from vehicle to controller?**
      Answer:
      Three types of the messages needs to be transmitted
      Accident Message (M1)
      Bad Road Message (M3)
      Construction Site Message (M4)
      This message will transmission happens to the all vehicles in proximity. Let it be m.
      Therefore, No of messages to be communicated = 3+m.
      Total time required to communicate this message = m*propogation cost of this 3 messages from vehicle to controller.

      Computation cost at Vehicle RSU and Controller
      Number of concatenation: 8
      Number of Encryption: 3
      Number of Hashing: 3
      Number of Decryption: 2

      Concatenation Computation Cost: 8*0.00015 = 0.0012 ms
      Encryption Computation Cost: 3*1.534 = 4.602 ms
      Hashing Computation Cost: 3*0.0083 = 0.0249 ms
      Decryption Computation Cost: 2*1.834 = 3.668 ms

      Computation Cost = 8.2961 ms

      Communication cost from Vehicle to Controller for M1, M3, M4
      Cost for message M1 (M1 size = 2bytes)
      - From Vehicle to RSU
        Key(Xk) size = 1 byte … Assumption
        P size = M1 size + IDv size + IDu size = 2 + 1 + 1 = 4 byte
        Q size = SHA256(P) = 1 byte … Assumption
        Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 4 + 1 = 6 bytes
        Total size = Timestamp + X = 1+6 = 7 bytes

      - From RSU to controller
        Key(Rk) size = 1 byte … Assumption
        Y = Size of P = 4 byte

Encryption Size (Z) = Key(Rk) size + Y = 1 + 4 = 5 byte
Total size = Timestamp + Y = 1+5 = 6 bytes

Total size = 7+6 = 13 bytes

Cost for message M3 (M3 size = 10 byte)

- From Vehicle to RSU
  Key(Xk) size = 1 byte … Assumption
  P size = M3 size + IDv size + IDu size = 10 + 1 + 1 = 12 byte
  Q size = SHA256(P) = 1 byte … Assumption
  Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 12 + 1 = 14 bytes
  Total size = Timestamp + X = 1+14 = 15 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 12 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 12 = 13 byte
  Total size = Timestamp + Y = 1+13 = 14 bytes

Total size = 15+14 = 29 bytes

Cost for message M4 (M4 size = 18 byte)

- From Vehicle to RSU
  Key(Xk) size = 1 byte … Assumption
  P size = M4 size + IDv size + IDu size = 18 + 1 + 1 = 20 byte
  Q size = SHA256(P) = 1 byte … Assumption
  Encryption Size (X) = Key(Xk) size + P size + Q size = 1 + 20 + 1 = 22 bytes
  Total size = Timestamp + X = 1+22 = 13 bytes

- From RSU to controller
  Key(Rk) size = 1 byte … Assumption
  Y = Size of P = 20 byte
  Encryption Size (Z) = Key(Rk) size + Y = 1 + 20 = 21 byte
  Total size = Timestamp + Y = 1+21 = 22 bytes

Total size = 13 + 22 = 35 bytes

Communication cost = (13+29+35)/250 = 0.308 ms

Time to transmit from Vehicle to Controller = m * (computation cost + communication cost)
Time to transmit from Vehicle to Controller = m * (8.2961+0.308)=8.6041ms

b. Also, explain which type of message will be transmitted first and why?
Answer:
As discussed above 3 types of message will be shared. The priority of Accident Message is higher than other 3 messages. Therefore, Accident message has to be

transmitted first followed by Bad Road Message and Construction Site Message. Also, during accident the drivers and other people who are injured need instant medical services. Therefore, to suffice this needs Accident Message is transmitted First.