Security And Its Application
Assignment 3

In this assignment we were provided with an IOV scenario and we needed to calculate the different costs. We also need to check whether the communication can withstand different kinds of attacks. The scenario basically consists of two phases: **registration and communication**.
The first part defines the registration between the RSU and IOV server. Whereas the second part defines the communication between the Vehicle to Vehicle and Vehicle to RSU respectively.

Answer 1: RSU Setup

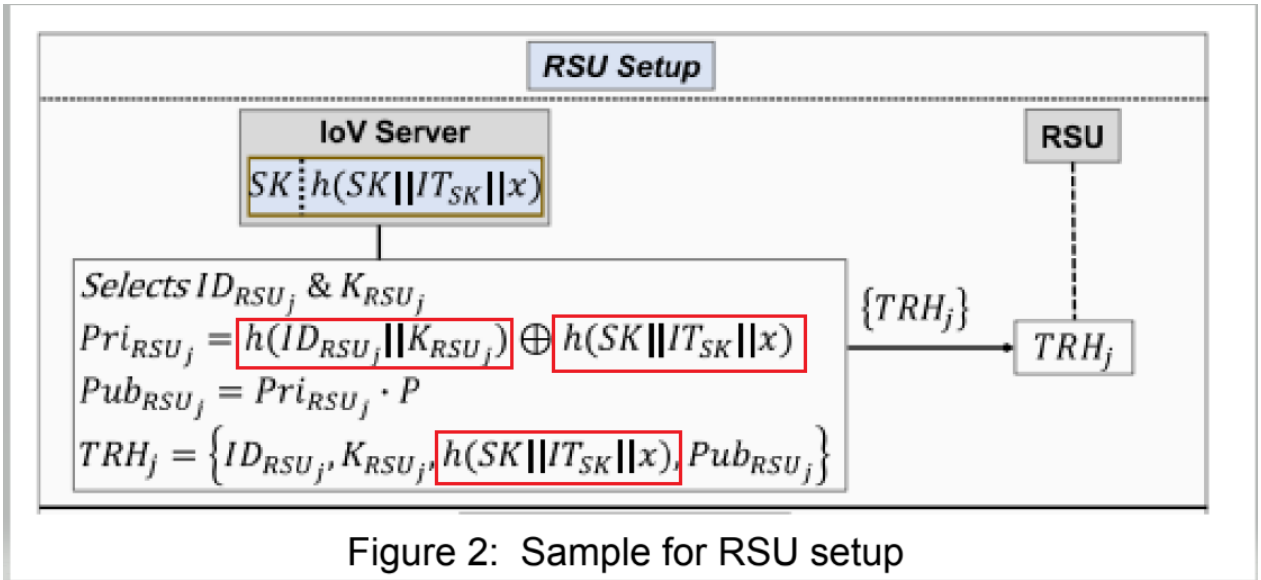

Figure 2: Sample for RSU setup

In the above-defined communication the sender is IOV and the Receiver is RSU. There are basically three different secure operations which are:

- One-way hash 256-bit SHA of **ID | | K** at the server.
- One-way hash 256-bit SHA of **SK | | IT | | x** at the server.
- Both of the above are used to calculate PRI.
- Then PUB is calculated as PRI * P
- One-way hash 256-bit SHA of **SK | | IT | | x** at the server to calculate the TRH.
- After this, the TRH is sent to RSU.

These operations are also highlighted in the above image.

Answer 2: Vehicle to Vehicle and RSU Data Transmission

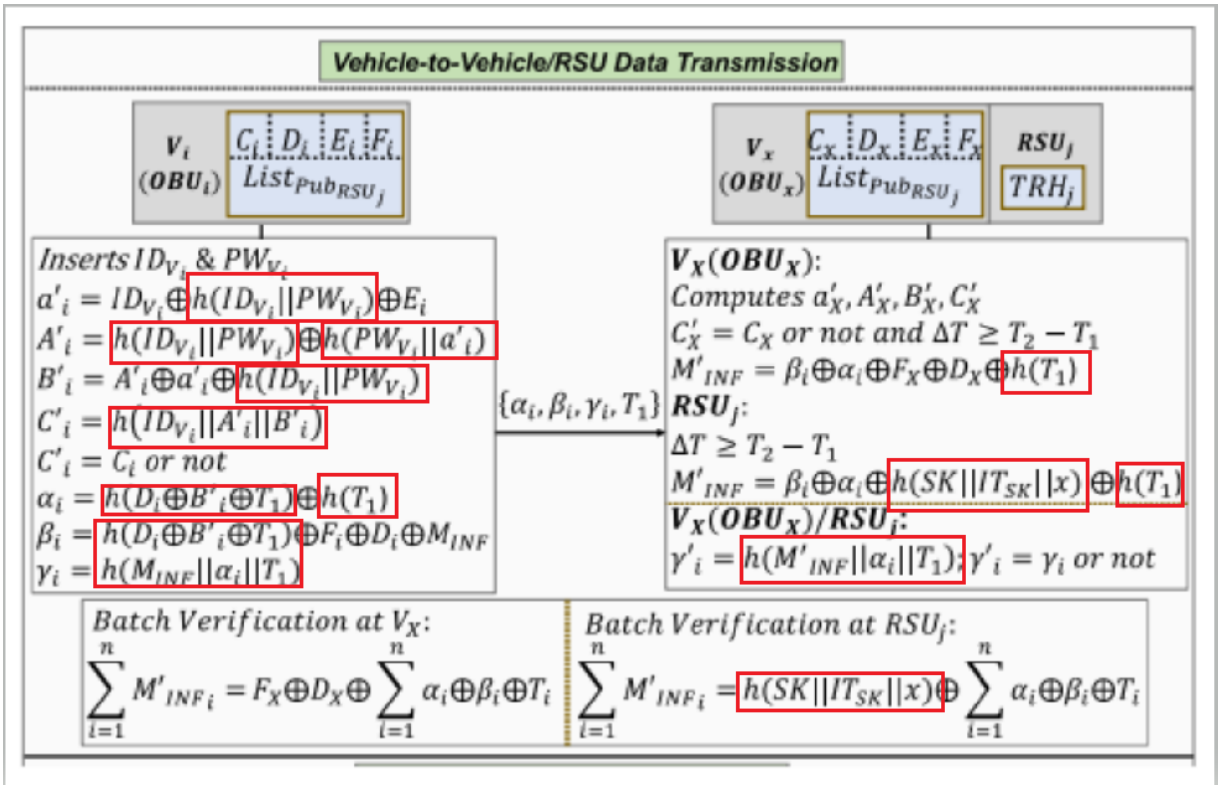

Figure 3: Sample for Vehicle to vehicle data transmission

In the above-defined communication scenario between the vehicle to vehicle or vehicle to RSU, there are some security operations which are.

At sender:

- One-way hash 256-bit SHA of **ID | | PW** at the Vi to calculate a'.
- One-way hash 256-bit SHA of **ID | | PW** xor with One-way hash 256-bit SHA of **PW | | a'** to calculate the value of A'.
- One-way hash 256-bit SHA of **ID | | PW** xor with A' and a' to calculate B'.
- One-way hash 256-bit SHA of **ID | | A' | | B'** to calculate the value of C'
- One-way hash 256-bit SHA of **D xor B' xor T1** xor with One-way hash 256-bit SHA of **T1** to calculate the value of Alpha.
- One-way hash 256-bit SHA of **D xor B' xor T1** xor with F, D, M to calculate Beta
- One-way hash 256-bit SHA of **M | | Alpha | | T1** to calculate gamma.

At Reciever (can be Vehicle or RSU):

- One-way hash 256-bit SHA of **T1**
- One-way hash 256-bit SHA of **SK | | IT | | x**
- One-way hash 256-bit SHA of **M | | Alpha | | T1**
- Also there are similar computations of a', A', B', C'.

These operations are also highlighted in the above image.

Answer 3:
Assumptions:

1. Assuming the values are secret and securely stored in the server and only the user knows.
2. Assuming the Hash functions are one-way SHS 256 bit hash functions with an execution time of 0.0382ms (given in the table).
3. Size of the output of hash variables is 32 bytes and other variables are 4 bytes.
4. Assuming the cost of Concatenation and Xor are 0.000005ms.
5. The heat generated for 1ms time is 1000 Micro-Joule
6. All the above assumptions are made randomly.

Execution time:
For RSU Setup:

S.No.	Operation	Number of Operation	Cost
1.	Hashes	2	2 * 0.0382ms = 0.0764ms
2.	Concatenation	3	3 * 0.000005ms = 0.000015ms
3.	Xor	1	1 * 0.000005ms = 0.000005ms
			Total = 0.07642

For Vehicle to Vehicle/RSU data Transmission:
For Vi - Vie:

S.No.	Operation	Number of Operation	Cost
1.	Hashes	7	7 * 0.0382ms = 0.2674ms
2.	Concatenation	6	6 * 0.000005ms = 0.000030ms
3.	Xor	13	13 * 0.000005ms = 0.000065ms
			Total = 0.267495

For the Vi - RSU:

S.No.	Operation	Number of Operation	Cost
1.	Hashes	3	3 * 0.0382ms = 0.1146ms
2.	Concatenation	4	4 * 0.000005ms = 0.000020ms
3.	Xor	7	7 * 0.000005ms = 0.000035ms
			Total = 0.114655ms

Storage Cost:
For IOV - RSU:

S. No.	Variable	Cost(Bytes)
1.	ID	4
2.	K	4
3.	SK	4
4.	IT	4
5.	X	4
6.	PRI	32
7.	P	4
8.	PUB	32
		Total = 88 Bytes

For Vi - Vj:
Vi:

S. No.	**Variable**	**Cost(Bytes)**
1.	ID	4
2.	C	4
3.	D	4
4.	E	4
5.	F	4
6.	PW	4
7.	a’	32
8.	A’	32
9.	B’	32
10.	C’	32
11.	ALpha	32
12.	Beta	32
13.	Gamma	32
		Total = 248

Vj:

S. No.	Operation	Cost(Bytes)
1.	C	4
2.	D	4
3.	E	4
4.	F	4
5.	M	32
6.	a’	32
7.	A’	32
8.	B’	32
9.	C’	32
10.	ALpha	32
11.	Beta	32
12.	Gamma	32
		Total = 272

RSU:

S. No.	Operation	Cost(Bytes)
1.	M	32
2.	Gamma	32
		Total = 64

Communication cost:

S. No.	Operation	Variables Communicated	Cost(Bytes)
1.	IOV to RSU	ID, K, h, PUB	4 + 4 + 32 + 32 = 72
2.	Vi-Vj/RSU	T1, alpha, beta,gamma	4 + 32 + 32 + 32 = 100
			Total = 172 Bytes

Energy Consumption:

S. No.	Operation	Time	Cost(Mico-Joule)
1.	IOV to RSU	0.07642	0.07642 * 1000 = 76.42
2.	Vi-Vj/RSU	0.267495 + 0.114655	0.38215 * 1000 = 382.15
			Total = 485.57 Micro-Joules

Answer 4:

1. Replay Attack:

In this attack, the attacker tries to send the modified message to the user that he has intercepted before.

In the defined scenario whenever there is a communication between the vehicle to vehicle or between vehicle to RSU a timestamp is used which is **T = T2- T1** which verifies the freshness and the arrival time of the message and when an attacker tries to perform the replay attack the value of time T is changed and thus the attack can be intercepted or can be found out. This is because the users have the value of T1 and T2 and thus they can verify the value of T and hence Replay Attack can be found and thus the scenario can withstand the attack.

2. Impersonation Attack:

In this attack, the attacker tries to impersonate a legitimate user and tries to get the information like the values of **C, D, E, and F** which are known to the user. And then calculates the fake values of other variables and sends them to other users illegally.

But in the scenario which is defined the values of alpha, beta, gamma, and T are dependent on the hash of the ID and PW which are secret to the user and the rest values are also dependent on this hash, and even if he has one value calculating the result with a single known value will not be possible hence we can say even if the attacker has the values of C, D, E, and F he will not be able to calculate the values of other variables and thus will not succeed in the attack.

3. Man in the Middle Attack:

In this attack, the attacker intercepts the communication between two legitimate users and also accesses the transferred data, and then the attacker modifies the data or drops some part of it.

But in a defined scenario even if the channel is insecure the message is calculated as **M = alpha EXOR beta EXOR F EXOR D EXOR** hash here the values of alpha, beta, and gamma are recalculated, and thus even if the attacker has the values of message and variables we can check whether the result will be the given message or not.

Thus the scenario can withstand the Man in Middle attack.

4. Modification:
In this attack, the attacker modifies the values sent from one user to another. Like in the defined scenario the values send are alpha, beta, gamma, and T. Now all of these values are the result of hashing and thus there is no way the attacker can guess the values of C, D, E, and F from these values, and hence he will not be able to change the message. Further, he has no access to the ID and PW as they are used in hashing Which makes modification even more difficult.
Thus the scenario can withstand the Modification attack.

5. Denial of Service attack:
In this attack, the attacker tries to deny the services provided to the user by using unethical ways like overflowing the server using requests and this can lead to accidents in case the user is not able to get critical information about the vehicle, etc. In the defined scenario the communication between the RSU and the vehicle is defined using alpha, beta, gamma, and T now if there is any case where the user is denied the service and the values of alpha, beta, gamma, and The have no way to get the message. But the cost of communication and storage is less and thus the scheme can withstand the Denial of Service Attack.

6. Password Guessing:
In this attack, the attacker tries to guess the password and by guessing the password tries to illegally use the account of the legitimate user. Now in the defined scenario, we know that it will be difficult for the attacker to access the Password of the user but in the worst case the server where there is a password stored may be hacked or the attacker gets a hint of the password which can help him to guess the password. Or it may happen that the uses some very advanced hardware that can perform computations very fastly and thus he can guess the password.
Thus the scenario may or may not withstand the Password guessing. But there is a strong reason that the scheme can withstand Password guessing.

7. Sybil Attack:
In this type of attack, the attacker tries to create multiple users and use these on the system but since our scheme is safe from impersonation attacks it should withstand a Sybil attack.

8. Hash Collision:
Since we use SHA 256 and it is known that SHA is collision-resistant thus the scheme is also collision-resistant.