CSE 4000

Weekly Presentation

Title: Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks

Presented by,

Mazharul Islam,

Roll-1807102

Date: 07-05-2023

1.What I studied

1. Methodology in details

2. Assumption and problem statements

3. Proposed Schemes

4. Analytical model

2. What I have learnt

1. AODV and AOMDV routing protocols

2. Enhanced Homomorphic Cryptosystem (EHC)

3. Secret key generation, Encryption and Decryption:

Secret Key Generation (K):

– $p, q \in P$, where P is prime, and $m = p * q$.

– Generate a random number r.

– The set of original plaintext messages $P = Zp = \{ x : x < = p\}$, $Zm = \{ x : x < m\}$ has the set of ciphertext messages.

– Secret values r, m and q

– Shared Key $K = p$.

Encryption (E):

– $x \in Zp$

– The ciphertext C is calculated as $y = Ep (x) = (x + r \times pq) \pmod m$.

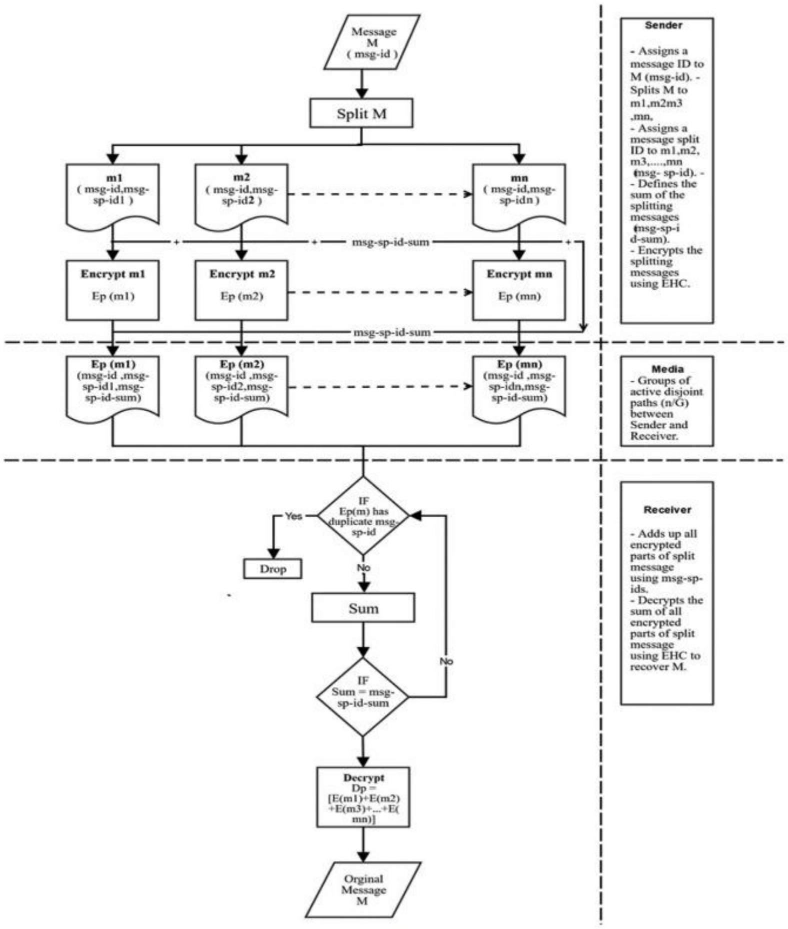
Decryption (D):

– The plaintext x is recovered as x = Dp (y) = y mod p.

4. Elliptic Curve Diffie-Hellman (ECDH) key transmission algorithm.

- Sender generates a random integer *a* as my private key
- Sender generates my public key *A* by computing *aG*
- *Receiver generates a random integer b* as your private key
- Receiver generates your public key *B* by computing *bG*
- *They exchange public keys*
- *Sender calculates K* as *aB*
- *Receiver calculates K* as *bA*

5. How proposed Scheme works.



- Assigns a message ID to M (msg-id). - Splits M to m1,m2m3 ,mn, - Assigns a message split ID to m1,m2, m3,....,mn (msg- sp-id). - - Defines the sum of the splitting messages (msg-sp-id-sum). - Encrypts the splitting messages using EHC.

- Groups of active disjoint paths (n/G) between Sender and Receiver.

- Adds up all encrypted parts of split message using msg-sp-ids. - Decrypts the sum of all encrypted parts of split message using EHC to recover M.

Fig. 2. The procedure of the proposed scheme.

6. Real Life Example:

The number of disjoint paths n = 6 between the sender and receiver.

• Number of groups () is G = n / two or more paths in each group G = 6 / 2 = 3

• The entire message M = 9.

• Parts of the entire message m = M / G = 9 / 3 = 3 where m is m 1 = m2 = m3

• The message's id for the entire message M is msg − id = 1.

• The message part ids for the message parts are msg − sp − id1 = 1, msg − sp − id2 = 2, and msg − sp − id3 = 3.

• So, the message part id's sum is msg − sp − id − sum = msg − sp − id1 + msg − sp − id2 + msg −sp − id3 = 1 + 2 + 3 = 6

• Encrypted the message parts m1, m2, m3 using EHC at the sender before sending them to the destination: We have M = 9 and m1 = m2 = m3 = 9/3 = 3

7. M/M/1 queue with FCFS.

3. Next week plan

1. Performance evaluation.

2. Conclusion.