Elliptic Curve Algorithm for Lightweight Cryptography in Mobile-Ad-Hoc Networks(MANETs)

Students:
Abdallah Masri
Mona Khammash
Rawan Tammam

Instructor:
Dr. Ahmed Awad

Outline

- Introduction
- Related Work
- Elliptic Curve Overview
- Elliptic Curve Cryptography
- Simulation Environment
- Results and Analysis
- Conclusion

Introduction

MANETs

- ❏ Decentralized type of wireless network.
- ❏ Nodes participation done by forwarding data from node to another.
- ❏ Continuously self-configuring, self-organizing, and infrastructure-less
- ❏ Ad hoc wireless networks are power constrained since nodes operate with limited battery.
- ❏ Lightweight cryptography used for MANETs to reduce power consumption, better performance, and efficient security.

Related Work

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s:

- Framework for QoS-aware secured end-to-end data communication in MANETs.
- New hybrid based algorithm named ECKCDSA with SHA 512 hash function.

- New approach of elliptic curve and hill cipher (ECCHC): The most important drawback is using the same the self-invertible key matrix will be generated, and the same key will be used for encryption and decryption .

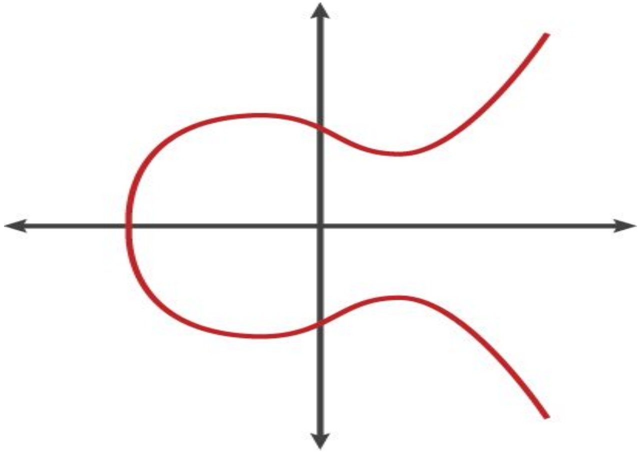
- HYPER ELLIPTICAL CURVE CRYPTOGRAPHY for key escrow in MANETs

Problem statement

- MANETs suffer from a lot of difficulties, challenges, limitations, and attacks.
  - The most important challenge is the **limited battery.**
  - We need to find an acceptable power consumption while maintaining the security level .
  - ECC achieves both high security level and reasonable power consumption.

Elliptic Curve Overview

- Elliptic Curve is a cubic curve, uses the Weierstrass equation: $y^2 = x^3+ax+b$.
- Elliptic curve is smooth, non-singular and projective,
- Line between two points on this curve will always intersect a third point (projective).



Elliptic Curve Overview

- We can compute *points* on the curve. A point is simply a pair (x, y) that satisfies the equation of the curve.
- From our elliptic curve, we can construct an algebra with operations known as *point addition*, point doubling, and *point multiplication*.

Elliptic Curve Cryptography

- Key-based technique for encrypting data.
- Pairs of public and private keys for encryption and decryption.
- These key-pairs rely on “Trapdoor Functions” which are easy to compute in one direction but much harder to reverse.
- ECC creates keys that are more difficult, mathematically, to crack.
- Maintain high levels of both performance and security.

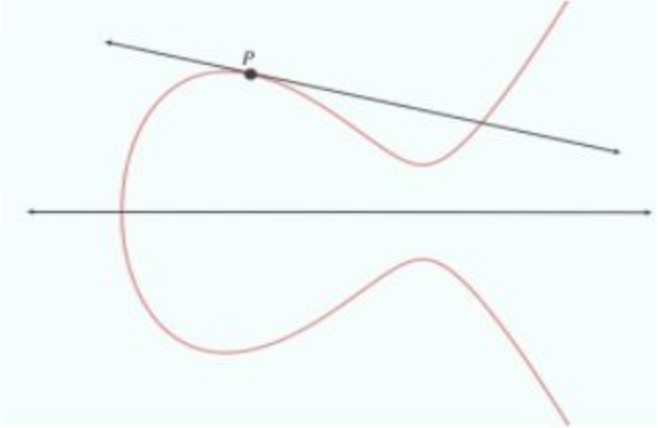
Elliptic Curve Cryptography

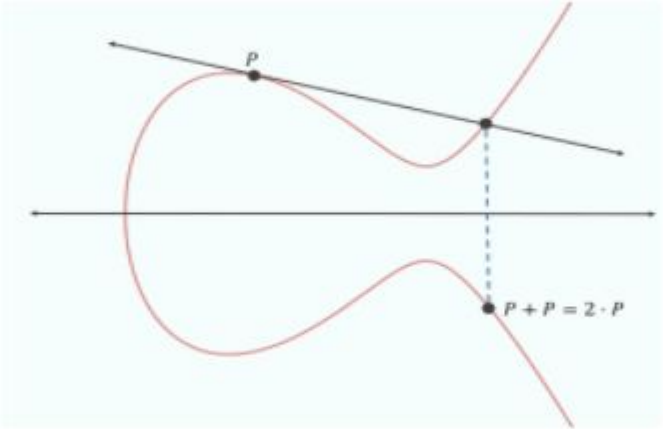
- RSA vs. ECC
  - The difference in size to security yield between RSA and ECC encryption keys is notable.
  - An elliptic curve cryptography key of 384 bit achieves the same level of security as an RSA of 7680 bit.
  - ECC uses less memory than RSA does.
  - RSA key size increases exponentially as security levels increase, ECC key lengths increases linearly.

RSA key length(bits)	ECC key length(bits)
1024	160
2048	224
3072	256
7680	384
15360	512

Elliptic Curve Cryptography- Point Multiplication

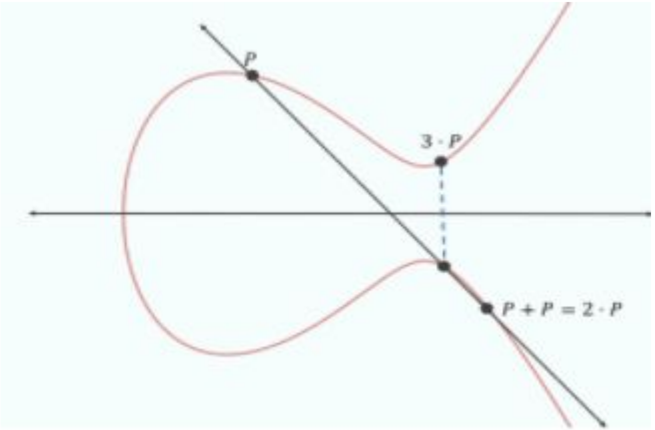
- Finding two unique points for encryption for the equation $y^2 = x^3+ax+b \pmod p$
- z.
  - Draw a line tangent from a starting point *P*, finding where it intersects the curve.
  - Flip the axis of the and get 2.*P*.





Elliptic Curve Cryptography- Point Multiplication

- Draw a line from 2.*P* through the starting point and find the new intersection point.
- Flip the axis and get 3.*P*.
- *Repeat n-times*.
- *Q = n.P with no obvious relation with P*.

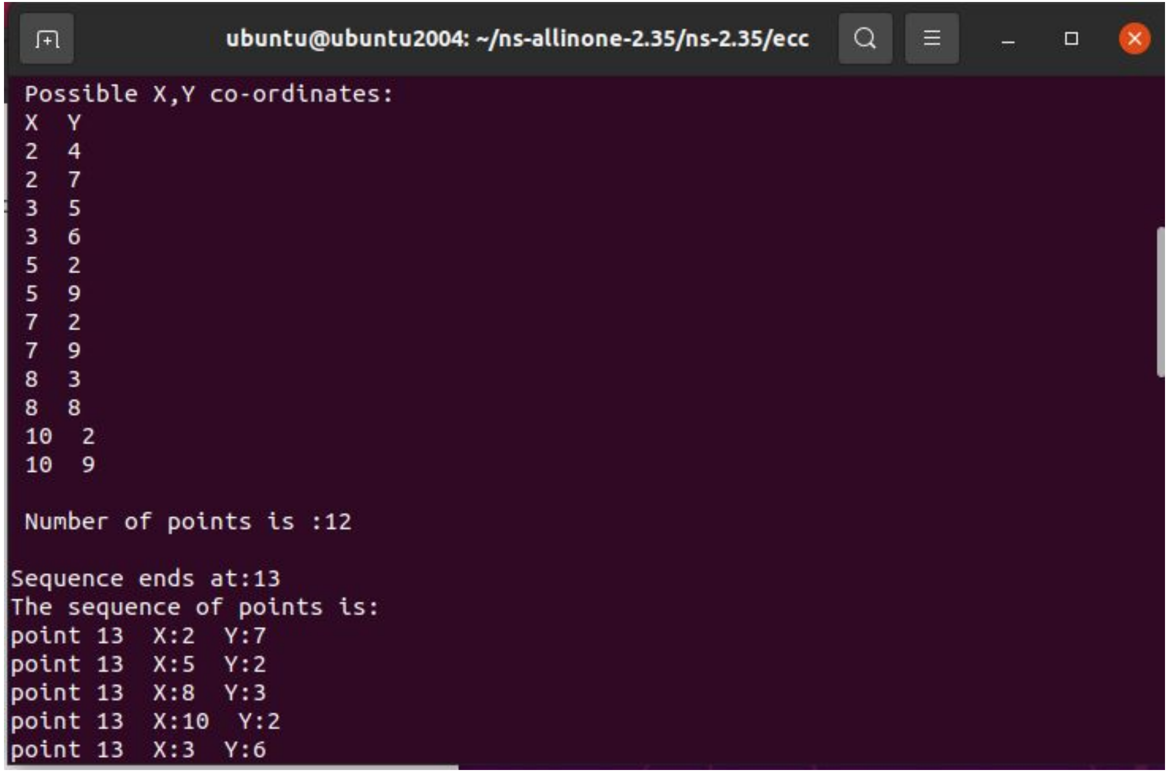


Elliptic Curve Cryptography

- Security
  - Ability to compute a point multiplication and the **inability to compute the multiplicand** given the original and product points.
    - Need to try all possibles n => effort that is computationally intractable if *n* is large.
    - The largest n possibility is the subgroup order.
  - The **size of the elliptic curve** which is determined by the prime number, determines the difficulty of the problem.

Elliptic Curve Cryptography

- Encryption



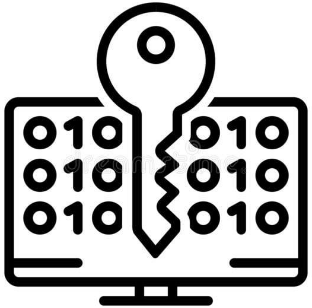
```
ubuntu@ubuntu2004: ~/ns-allinone-2.35/ns-2.35/ecc
Possible X,Y co-ordinates:
X  Y
2  4
2  7
3  5
3  6
5  2
5  9
7  2
7  9
8  3
8  8
10  2
10  9

Number of points is :12

Sequence ends at:13
The sequence of points is:
point 13  X:2  Y:7
point 13  X:5  Y:2
point 13  X:8  Y:3
point 13  X:10  Y:2
point 13  X:3  Y:6
```

Elliptic Curve Cryptography

- Encryption
  - Choose random point P for public key.
  - Choose random k, calculate Q = kP where k is the private key.
  - Set X0 from Q.
  - Calculate y1 = PointCompress(P)
  - Calculate y2 = x * x0 % P, where x is the data and p is the prime number used.
  - Ciphertext = (y1,y2)

Elliptic Curve Cryptography

- Decryption
  - Calculate PointDecompress(y1)
  - Multiply resultant with private key *k*.
  - Take resultant x coordinate value as X0.
  - Calculate y=y2*(X0)-1 % p



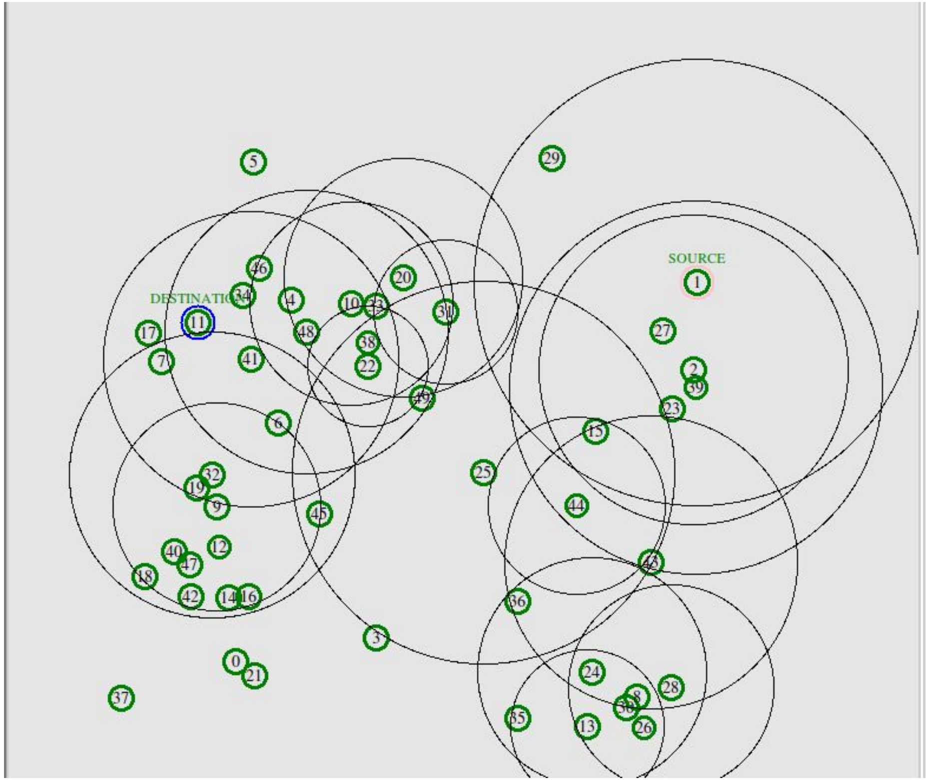
Simulation Environment

- We used the following NS 2.35 settings

Parameter	values
Simulator	NS 2.35
Number of Nodes	50
Node Speed	20ms
Simulation Area	600m x 600ms
Simulation Time	10s
Routing Protocol	AODV
MAC Type	802.11
Antenna Model	Omni Antenna
Radio Propagation	Two Ray Ground
Interface Queue Type	Drop Tail

AODV (Ad-hoc On-demand Distance Vector).

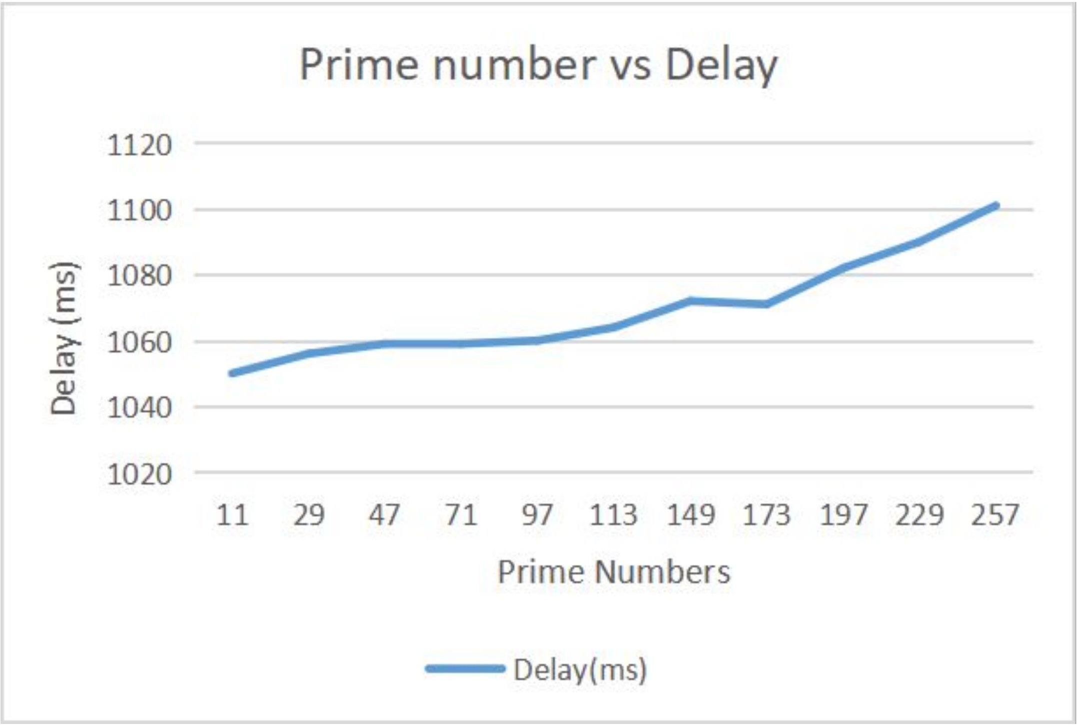
Simulation Environment

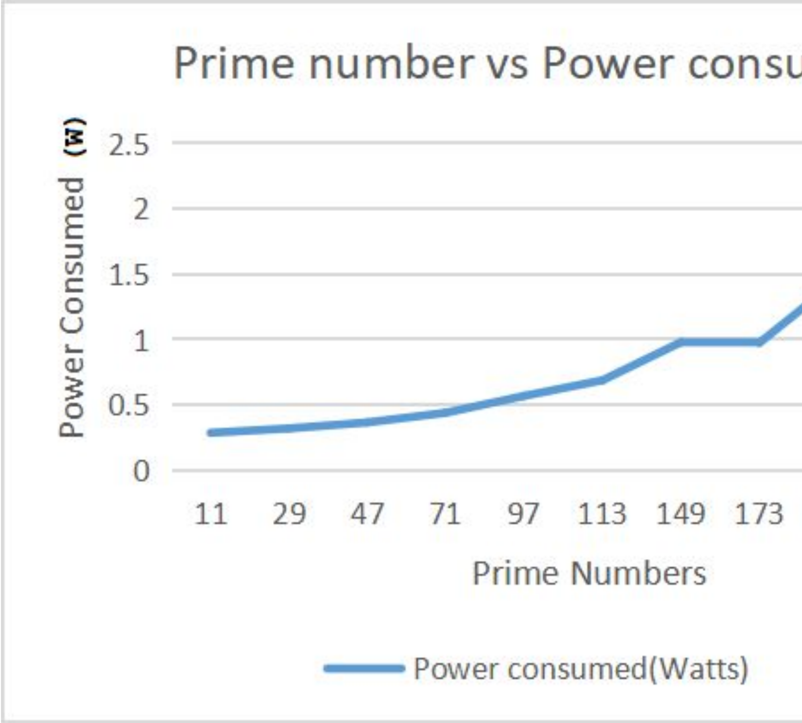


Results and Analysis

- Performance and Security metrics.
  - End-to-end delay : Time taken for a packet to be transmitted across a network from source to destination.
  - Power Consumed: The amount of power loss in the node.
  - Subgroup Order: The largest n possibility in choosing the points before a cycle appears.

Results and analysis





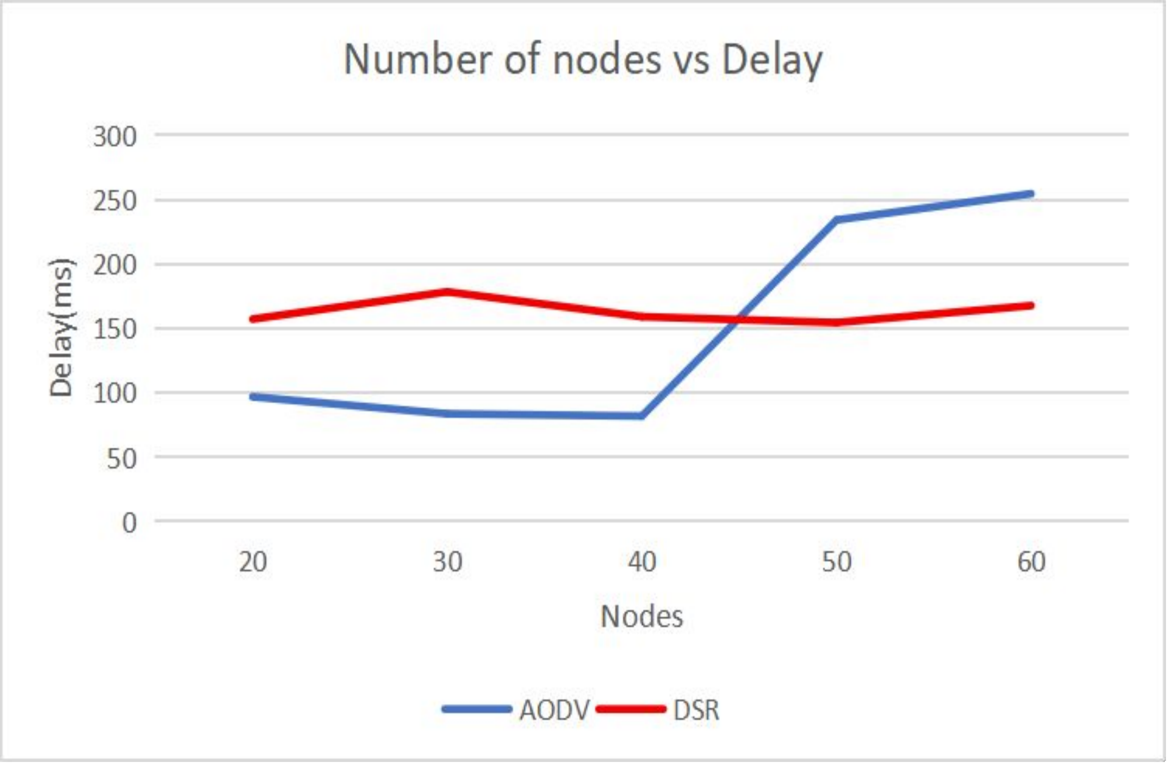
Results and analysis

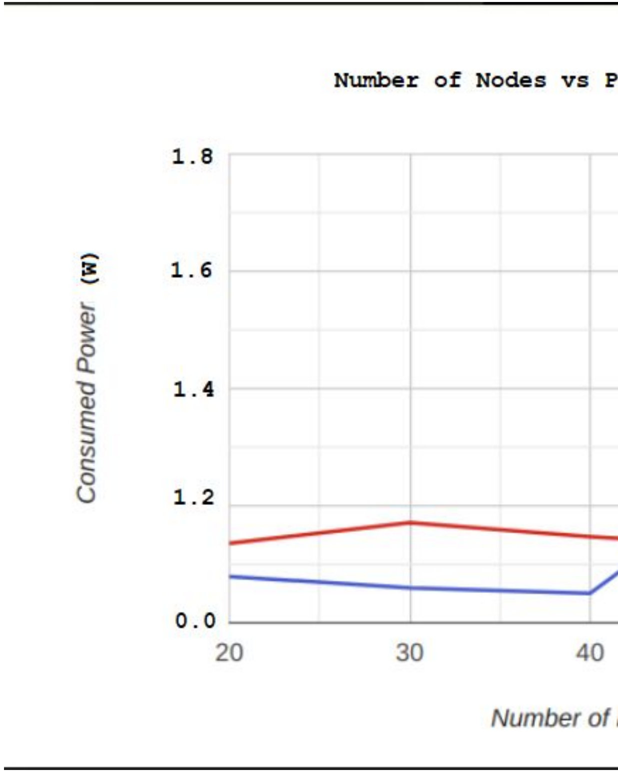
p	Subgroup Order	Consumed Power(W)
11	13	0.2868
29	38	0.3203
47	52	0.3661
71	54	0.4401
97	58	0.5690
113	117	0.6887
149	171	0.9796
173	160	0.9740
197	205	1.4549
229	209	1.7884
257	240	2.2076

Results and Analysis

- AODV routing protocol performance was poor.
- We need to find a fitting protocol to suit EEC.
- Dynamic Source Routing (DSR)
  - similar to AODV in that it forms a route on-demand when a transmitting node requests one.

Results and Analysis





Conclusion

- The chosen Prime number must achieve a high level of security in MANETs with a reasonable consumed Power.
- It is recommended to use DSR routing protocol due to its higher performance with minimal delay and acceptable communication power consumption.

References

[1] https://opus.lib.uts.edu.au/bitstream/10453/127459/4/journal-04042018_Sean.pdf?fbclid=IwAR0XZbo3z4pwDJ9cO4O5aTSf0BVSft3yQG73C4oQHUvCXfp8x6-yqsAMaEE

[2] https://www.irjet.net/archives/V3/i6/IRJET-V3I6331.pdf

[3]https://www.researchgate.net/profile/Omar_Almomani2/publication/343163452_A_new_hybrid_text_encryption_approach_over_mobile_ad_hoc_network/links/5f19bae545851515ef449dac/A-new-hybrid-text-encryption-approach-over-mobile-ad-hoc-network.pdf

[4] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3565146

Thank you

Any Questions?