Waseda University Graduate School of Fundamental Science & Engineering

Department of Computer Science and Communications Engineering

Evaluation of RSA and ECDSA Applying for Information Centric Networking

(30 / January /2017)

Pariwash Foushanji

5115fg10-5

Supervisor

Takuro SATO

Acknowledgement

First of all I want to thank God for giving me the ability to complete my master's program Successfully. Then I would like to express a deep sense of thanks to my supervisor professor Sato Takuro for his great assistance and instruction during my master course in choosing the research direction and writing my master thesis.

I would like to thank all professors of Graduate school of Fundamental Science and Engineering during at Waseda University, for teaching and instructing me during my master course. Also great thanks from PEACE Project (Promotion and Enhancement of Capacity for Effective Development) of Japan for providing me master scholarship and giving me a great opportunity to come to Japan and increase my knowledge and experiences.

Last but not the least, I am grateful to my late Parents for all their efforts, prayers and supports that gave me the strength to progress in my life.

Table of Contents

Chapter 1 5

Overview of Information Centric Networking (ICN) 5

1.1 Introduction 5

1-2. Why ICN is More Robust in Compression to TCP /IP for Encryption and Network Security? 8

1-2-2.Infromation Centric Network Research Project 12

Chapter 2 13

2-1.An overview of security in Information Centric Networking Project 13

2-2. NDN Security: 14

2-3.DONA Security: 15

2-4.NetInf Security: 16

2-5. PURSUIT Security: 17

Chapter 3 18

3-1.Encryption and Decryption 18

3-2.Symmetric Encryption 19

3-3. (AES) Symmetric key Advanced Encryption Standard 20

Chapter 4 22

4-1. Asymmetric Encryption 22

4-2.Performance Comparison of RSA and ECDSA for Information Centric Network 23

4-2-1.RSA 23

4-2-2. Elliptic Curve Digital Signature (ECDSA) 25

Chapter 5 :Simulation and Experiential result 28

Chapter 6 33

Conclusion and Discussion 33

6-1:Elliptic Curve Digital Signature Algorithm Efficient Encryption and Decryption Algorithm Over Information Centric Networking 33

6-2 Conclusion 35

6-2 Future work 36

List of figures

Figure 1.1:ICN hourglass architecture with content chunks 6
Figure1. 2: ICN hourglass architecture of Interest packet and Data packet........ 7
Figure 1.3.TCP /IP header 9
Figure 1.4: Ipv6 header.. 10
IPv6 Authentication Header 10
Figure 1.5: Changing 1Pv6 header.. 10
Figure1. 6: IPv6 authentication header 10
Figure2.1:NDN overview 14
Figure2.2:DONA overview 15
Figure2:3.Netinf overview... 16
Figure2.4:PURSUIT overview 17
Figure1-5: Simulation result of time for RSA with key length
512,1024,2048,4096... 29
Figure 2.5: Simulation result of time of time for RSA with key length
512,1024,2048,4096... 30
Figure 3.5 : Simulation result of time for ECDSA with key length
160,192,224,265,348 and 512 for singing and verifying 31
Figure 4.5:Simulation result of time for ECDSA with key length
160,192,224,265,348 and 512 for key generation. 32

Chapter 1

Overview of Information Centric Networking (ICN)

1.1 Introduction

Computer network is becoming a major tool for establishing communication between people, devices, machines as well as things around the world. Computer networking that we use today started with ARPANET in late 1960's and early 1970's, which connected 4 computers around the USA for military proposes. The TCP/IP protocol, which was developed in the 1970 is known as the backbone of today's Internet and networking protocol and its communication language. The base of TCP/IP is related (DARPA) projects of united state. The main focus of TCP/IP on that time was to connect military resources as first network together in year 1985. After that Internet and networking attracted attention of commercial industries and on the workshop which was held at the same year 250 commercial industry attended to use Internet and networking. It was the first step of TCP/IP from military proposes to commercial industry [1,2]. After that computer networks find it is way to business and people social life, a great change has happened in the world. The basic requirement from the Internet at first was that how the data packets are forwarding among small number of computers. Information and communication technology have change the wary of communication between people. Usage of ICT in wired and wireless in different aspect of life has increased the users and number of data. TCP/ IP protocol talks about host-to-host communication based on named host [2].

When Internet usage starts widely and globally TCP/IP architecture faced with many different problems such as it is architecture and security of the end point. TCP/IP cannot fill today's users needs and a new alternative proposed for TCP/IP, which is Information Centric Networking. The architectures of Internet that today we use it's designed to connect few hosts on different geographically area and communication between host to host established via pipes with the model of client. It was an excellent match for client – server applications like HTTP, FTP, telnet and SMTP. From all information about TCP/IP protocol we can calm that TCP/IP protocol communication is based on infrastructure. But the new architecture Information Centric networking talks about content and information rather than infrastructure or communication between host-to-host [3]. The current Internet TCP/IP was not design to support content distribution over network and it is based on host-to-host communication; in contrast (ICN) Information Centric Networking has architecture that content delivery is based on name.

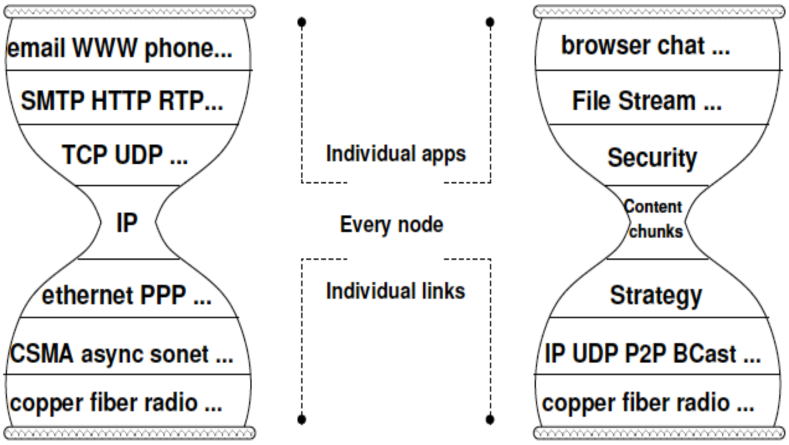

Figure 1.1:ICN hourglass architecture with content chunks

Based on new model of ICN hourglass, IP departs from ICN in deferent ways. The most important different is, security and strategy. In ICN, it is possible to have more connectivity rather that one. ICN offers security of the content, it means contents are secure itself and security is not based on communication pipe rather than the connections over which it travels.

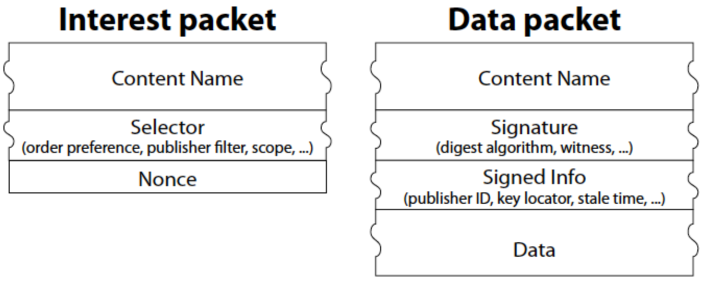
Interest packet
Content Name
Selector
(order preference, publisher filter, scope, ...)
Nonce
Data packet
Content Name
Signature
(digest algorithm, witness, ...)
Signed Info
(publisher ID, key locator, stale time, ...)
Data

Figure1. 2: ICN hourglass architecture of Interest packet and Data packet

The consumers or data drives ICN communication. ICN has two packet type which Interest and Data, the method of communication in ICN is based on consumers. As and example when a consumer wants to ask for a data, first the consumer sends a broadcast for interest on over all connectivity which are available, then the consumer receive the response with a data packet from the node that satisfies with Interest which was broadcast [4]. ICN forwarding engine has three data structure, which are forwarding, Information base, content store or buffer memory and pending Interest table. Focus and fundamental component of ICN as new paradigm are as Security, Mobility, Flexibility Scalability, and Cost- effective.

1-2. Why ICN is More Robust in Compression to TCP /IP for Encryption and Network Security?

TCP/IP protocol is known as host centric networking, which provides host-to–host communication, but in contrast information centric networking connecting people with content. At first security was not a primary concern for TCP/IP, and users simply trusted each other, but after the growth of Internet security of the end Point host become the main problem for TCP/IP Protocol, one of the major challenges that TCP/IP protocol faced was lack of packet authentication, because when if there I no authentication there is no grantee f or the packet. As IPV4 didn't use authentication to solve TCP/IP security problem, many different solution were used such as, firewalls, wrappers, Kerberos and SKIP [5].

Different attack on TCP/IP Protocol:

- TCP”SYN”attack
- IP spoofing sequence gassing
- Source routing
- Connecting routing & Connecting Hijacking
- DE synchronization during connecting establishment & DE synchronization in the middle of a connection
- Routing attack
- ICM P attack, DNS attack and lack of unique identifiers

16-bit source port number	16-bit destination number
32-bit sequence number	
32 bit acknowledgement number	
Header length and flags	16-bit widows size
16 –bit TCP checksum	16-bit urgent pointer
Options (if any)	
Data (if any)	

Figure 1.3.TCP /IP header

On the year 1990, TCP/IP security problems were questioning that attracted researchers attention TCP/IP security challenges raised finally a new version of protocol proposed which was IPv6. The main focus of the new version was on routing and security. Authentication and encryption problem of TCP/IP protocols were solved by the rise of IPv6.

Elements of IPv6 are as bellow.

- Header for Routing
- Header for Encryption
- Header for Authentication
- Header for Destination option
- Header for Hope by Hope

Version	Priority	Flow Label
Payload Length	Next Header	Hop limit
Source Address		
Destination Address		

Figure 1.4: Ipv6 header

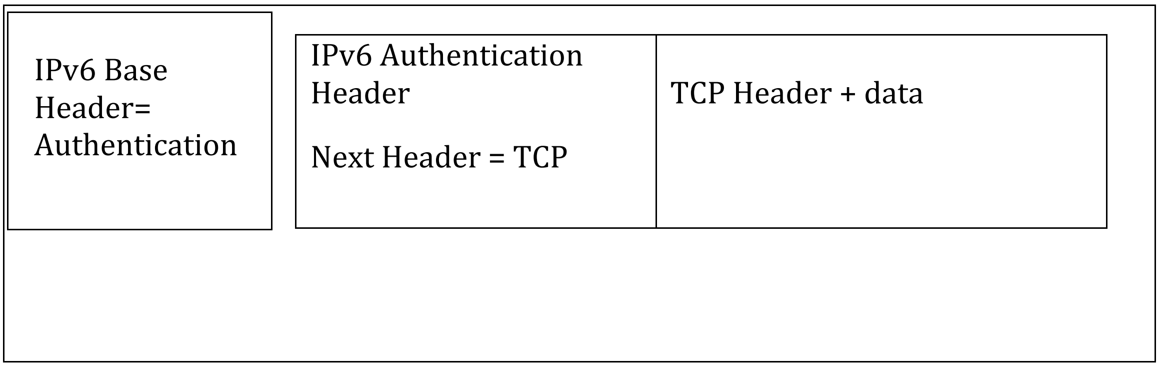

Figure 1.5: Changing 1Pv6 header

Next Header	Length	RESERVED
Security Parameters Index (SPI)		
Authentication Data		

Figure1. 6: IPv6 authentication header

Rise of IPv6 protocol has been solved security problems of TCP/IP but not all, the question that plagued researchers was that how to select the encryption between application and link level encryption .The main reason behind this question was that with the fast growing of network and use of encryption may slow down the protocols, and it will have negative effect on bandwidth [5]. In comparison to TCP /IP, ICN security has been changed from security the path to security the content. Security of the Content is much more important than security of the infrastructure [4]. ICN has the notion of content-based security, ICN provides authentication and digital signature for security and privacy of all content and in addition private content is protected with encryption [4]. More over, ICN paradigm inherently supports several security and privacy features such as provenance and identity privacy, which are still not effectively available in the host centric paradigm [6].

1-2-2.Infromation Centric Network Research Project

Different projects are basing ICN and their main focus is Internet architecture design, bellow projects target is to find problems and barriers of the host -to-hos model [7].

- DONA, Data Oriented Network Architecture form UC Berkeley.
- NDN, Named Data Networking, based on CCN from PARC.
- Named Node Network from Waseda
- PURSUIT, Publish Subscribe Internet Technology based on PSIRP

  Funded by EU frame work7 program.
- NetInf, Network of Information,
- SAIL, Scalable and Adaptive Internet Solutions
- COMET, Content Mediator Architecture for Content Aware Networks,
- CONVERGENCE

The main focus of ICN projects are on Information Naming, Information Delivery Information Mobility and Information Security. It means that information addressed and it is independent from location, there for information located anywhere in the network [7]. Host mobility In ICN is addressed by employing the publish/subscribe communication. Users have interest in information subscribe, they donate their interest to the network, many security problem of the Internet are widely du to disconnection between information semantics at the application as well as to the opaque data in individual IP packets [4].The concept of end-to-end security made it very difficult to place security and truest in the network. The new paradigm Information Centric Networking architectures add and indirection point between request of users for a piece of information decupling communication between users and the decupling process is a step toward against denial of services attack.

Chapter 2

2-1.An overview of security in Information Centric Networking Project

The main focus of ICN is on content retrieval form a network. In ICN, securing the content itself is much more important than securing the infrastructure or endpoints [8]. ICN architecture as a new paradigm consists of two new layers, which are strategy and security. In ICN paradigm security is not bound to the end point instead it secure content it self. Contents are authenticated with digital signature they are protected with encryption [4] one of the main reasons that ICN is more secure than IP is that ICN has authenticated from names to content [4].

2-2. NDN Security:

NDN security depends on the content publisher it provides signing of data packets with Cryptographically signing of each data packet and for the data integrity it uses hierarchically name space for which had effect on better routing and scalability. All the contents are singed with (PK) publisher's key. Different ways are used for verifying the key in NDN especially information through a friend, trusted third party, direct information Or information through a global PKI[7].

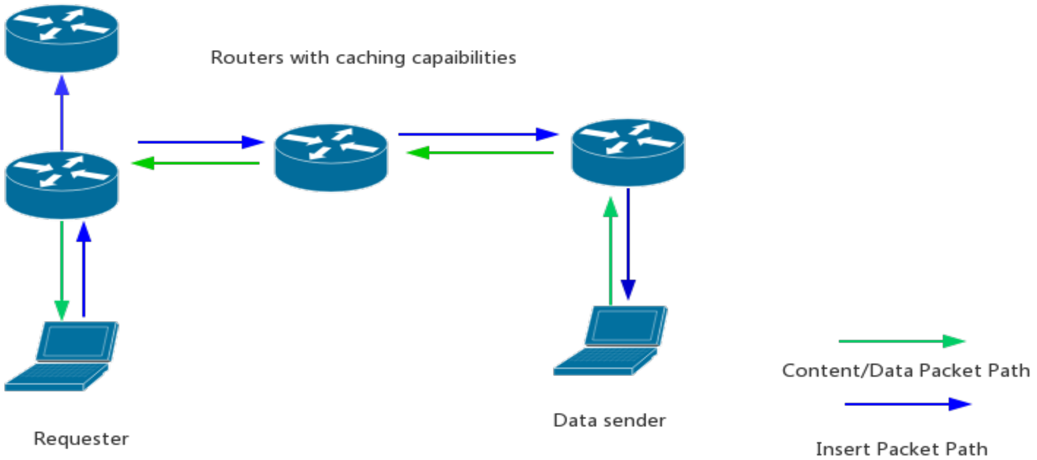

Figure2.1:NDN overview

2-3.DONA Security:

DONA uses the self-certifying name space providing name data integrity, the name data integrity method escapes necessity of PKI, and it is based on adding cryptographic hash function in Object level. Self-certifying names omit the need and requirement of a PKI with comparison of the data identify in data request, and it makes the security process a bit more simple [7].

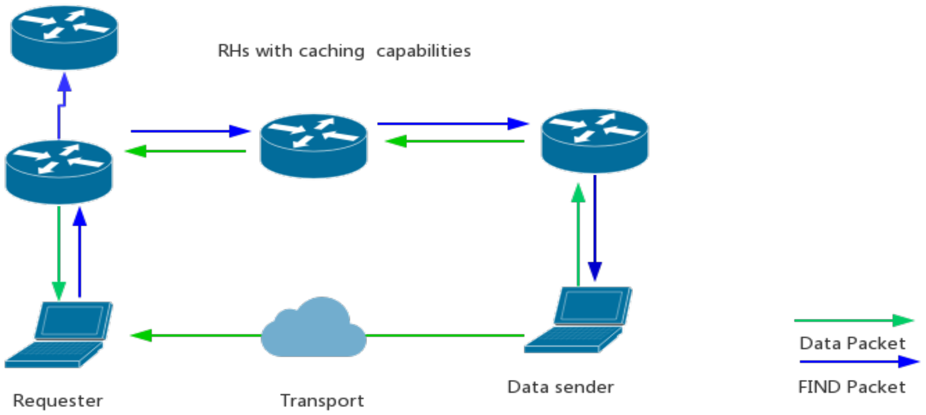

Figure2.2:DONA overview

2-4.NetInf Security:

NetInf uses the self-certifying name space for security. It can provide static and dynamic security based on object security. Naming format and the object model plays an important role for data integrity and validation .In netInf object security is provided with public key cryptography [7].

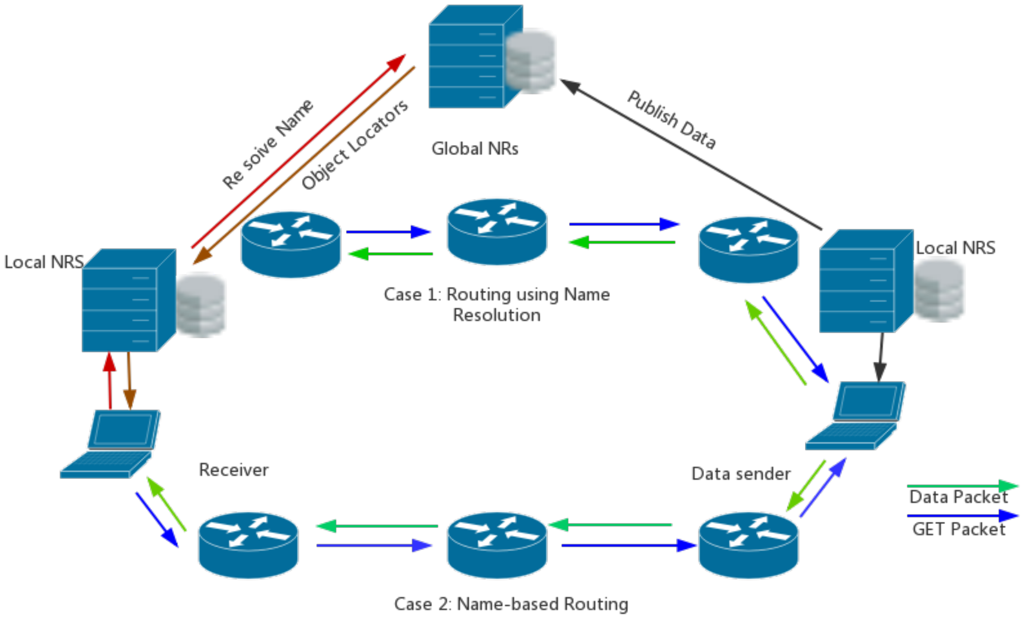

Figure2:3.Netinf overview

2-5. PURSUIT Security:

In PURSUIT Security is bond to the design for avoiding insecurity over network. PURSIT is using self-certifying name that release needs for PKI; this process make easy for nodes to check the name-data integrity when it receive data's name. One of security goal is preventing of unwanted traffic on both rendezvous and forwarding layers, PURSUIT uses elliptic-curve cryptography (ECC) for signature verification as well as packet-level authentication (PLA) for providing confidentiality, authenticity, and accountability on network layer [7].

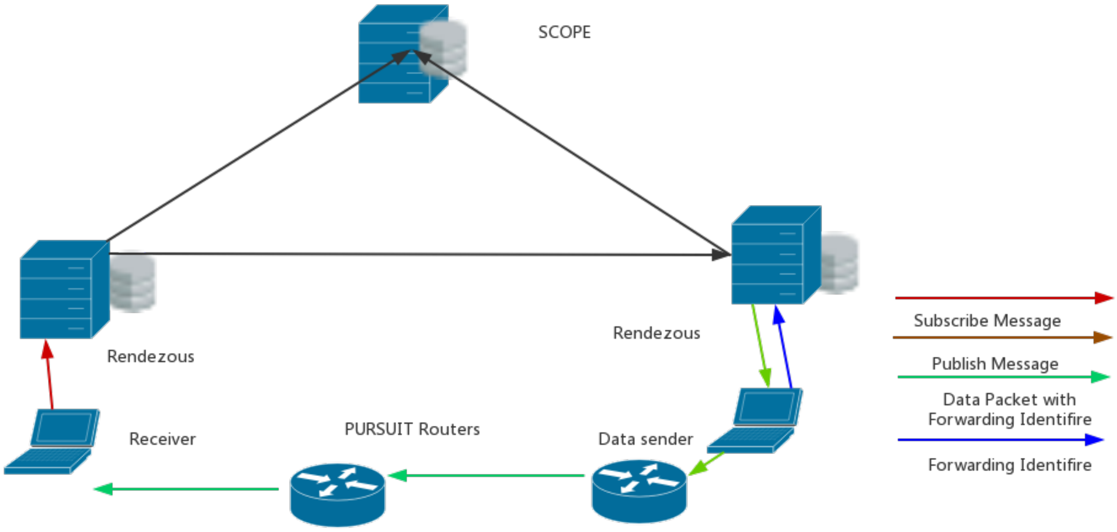

Figure2.4:PURSUIT overview

Chapter 3

3-1.Encryption and Decryption

In cryptography Encryption is called for process, which a massages is encoding in a secure way that no one can access but only the authorized parties. At first encryption used by military and government but now it is commonly used in protecting information. Beside encryption some other techniques are also needed to protect the integrity and authenticity of a massage, like verification of massage authentication code (MAC) or digital signature. Decryption is the revers of encrypted text to its original. In other word, decryption is the process of transforming data that has been unreadable through encryption back to its encrypted form. Decryption is the revers of encryption, decryption converts the unreadable data back to its original a Decryption may be accomplished manually or automatically .It may also be performed with a set of keys or password. Here we want to explain briefly about two kind of Encryption.

1-**Symmetric Encryption**

2- **Asymmetric Encryption**

3-2.Symmetric Encryption

Symmetric Encryption algorithm uses the same key for encryption and decryption of a plain text it means the same cryptographic key for both encryption of plaintext and decryption of cipher text. Symmetric key is also called, secret key or single key encryption for the first time it was propose on year 1970s [9].

Symmetric key encryption consist of bellow parts:

- Plain text: Input of an original data
- Encryption Algorithm: Is a process of converting plain text to cipher text.
- Secret key: A single key for encryption a plain text and decryption a cipher text.
- Cipher text: A simple text, which is converting and is no more the original one.
- Decryption Algorithm: A process of converting cipher text to original one

Bellow we listed famous Symmetric Encryption

- Towfish
- Serpent
- AES(Aka Rijendel)
- Blow fish
- CAT 5
- RC4 and IDEA.

3-3. (AES) Symmetric key Advanced Encryption Standard

One of the famous symmetric key encryption is AES which has three block cipher AES 128,AES-192-AES 256 adapted from a large collection originally published as Rijaneal each of these ciphers has a 128,192 and 256 bits, respectively. The Rijendael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.The AES cipher is specified as a number of repetitions of transformation round that convert the plaintext in to the final of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. Sets of reverse round are applied to transform cipher text back into the original plain text using the same encryption key .AES has blocked size of 128 bit and its key size is 128,192,256 bits, AES algorithm operate based on 4×4 matrix of bytes In AES the number of repetitions of transformation rounds convert plain text to cipher text [10]. AES algorithm with the three block of 128,192,256 is efficient to secure classified information up to the secret level .Top secret information might need either the 192or 256 key lengths. Symmetric Algorithm has it's own pores and cons.

1- No time delay as a result of the encryption and decryption.

2- Symmetric cryptography is able to provide a degree of authentication because data encrypted with one symmetric key cannot be decrypted with another symmetric key.

3- The major drawback of secret-key cipher is exchanging the secret key because any Exchange must retain the privacy of the key. This usually means that the secret key must Be encrypted in a different key, and the recipient must already have the key that will be Needed to decrypt the encrypted secret-key. This can lead to a never-ending dependency on another key.

4- In symmetric encryption each end has one copy of the secret key it means the key is exchanging over internet or large network and the probability of falling in the wrong hands or third party is high, because any one who knows the secret key can decrypt the massage.

Chapter 4

4-1. Asymmetric Encryption

The idea of Asymmetric Encryption or Asymmetric Cryptography Raised in year 1970 from Martin Hellman,Whitfield Diffie, independently, Ralph Merkle[11].The idea behind asymmetric cryptography was that how to solve the key exchange problems and to avoid key distribution. Researchers changed the secret key with a pair of mathematically related keys, public key and private key (secret key). Public key is available publicly, and individual who generated the key pair keeps private key secret [11].

Example: Bob generates randomly a public/private key pair that every one can access to the public key of Bob, as well as Alice, when Alice wants to send secret information to Bob; she encrypts the data using asymmetric algorithm and the public key generated by Bob. After that Alice sends the resulting cipher text to Bob, in this Cause no one is a bit to know the matching secret key and no one can convert the cipher text that Alice send to Bob, instead Bob can easily convert the cipher text of Alice to plain text. Because Bob has the matching secret key.

4-2.Performance Comparison of RSA and ECDSA for Information Centric Network

Network security and cryptography talks about how to protect information in digital form and how to provide security services [11]. With the rapid growth of information technology and comprehensive application of information equipment, information security becomes very important issue. Digital signature is one of the techniques that provide information safety [12]. Digital signature is a number dependent on some secret know only to singer, and, additionally, on the content of the message being signed [11].

4-2-1.RSA

RSA algorithm is called asymmetric or public key cryptosystem. Security of RSA is related to the large number prime factorization [13].

RSA Algorithm Process:

1- Two prime and random number generations P, Q of length K/2 bit.

2- Public key = P*Q (public key length is k-1).

3- Random encryption key generation, key E,

2<=key E<=Φ (n-1), GCD (key E, Φ (n))=1;

Key E*key D mod Φ (n)=1

Φ (n) is known as the Euler function of n, the value is

Φ (n)=(P-1)*(Q-1)

4-Calculate the decryption key, key=key E-1 mod (n)=1 key E-1 is inverse for the decryption key D mod Φ (n)=1

For encryption and decryption process form plain text to cipher text.

Encryption: c=M key E mode public key, in which M is plain text C is cipher text.

Decryption: M=C key D mod public key; n which M plain text, C is cipher text [13].

4-2-2. Elliptic Curve Digital Signature (ECDSA)

The Elliptic curve digital signature algorithm is known as the elliptic curve analogue of the digital signature algorithm. It has the application of Elliptic curve cryptography for digital signature generation and verification. Security of Elliptic curve digital signature depends on the Elliptic Curve Discrete logarithm problem. Elliptic curve digital signature uses three steep. Key pair generation, signature generation and signature verification. Security of ECDSA depends on the elliptic curve discrete logarithm problem (ECDLP)[14].

Process of ECDSA algorithm

A- The Key Pair generation of ECDSA

1. A random integer selection d in the interval [0,n-1].
2. Computing of Q=d×G , by point Multiplication.
3. Q,G elliptic curve points.
4. In (d,Q) d is Private Key and Q is Public key.

B-Signature Generation

1. Select the random integer k, 1≤ k≤n-1

   And compute
2. k×G =(x1, y1) and r=x1 mod n. If r = 0 then return to step 1
3. k^{-1}
4. $z=h-1(M)^2$
5. Calculate $s = k^{-1}(z+d\times r)$ mod n .If s=0 then returns to step 1
6. Signature for message hash z is (r,s)

C-Signature Verification

Receiver exploiting following steps can verify authenticity of the received message:

1. Verify r,s are in the interval[1, n-1].

   And compute

2. $z=h^{-1}(M)$.
3. $w= s^{-1}$ mod n.
4. $u1=z\times w$(mod n)and $u2=r\times w$(modn).
5. X=u1G+u2Q.If X=O∞
6. v=x1 mod n where X=(x1,y1).
7. Accepts the signature if and only if v=r [15].

RSA Parameters

Key length bits	RSA-512	RSA-1024	RSA-2048	RSA-4096
Sing per key size	0.000148s	0.005059s	0.002674s	0.0155568s
Verify per key size	0.00011s	0.00025s	0.000068s	0.000223s

Key length	RSA-512	RSA-1024	RSA-2048	RSA-4096
Key generator (sec)	0.112	0.232	1.322	1.112

ECDSA parameters

Key length bits	ECDSA 160	ECDSA192	ECDSA 224	ECDSA 256	ECDSA 384	ECDSA 512
Sing per key size	0.0001	0.0001	0.0002	0.0002	0.0004	0.0004
Verify per key	0.0005	0.0005	0.0007	0.0009	0.00019	0.0022

Key length bits	ECDSA 160	ECDSA 190	ECDSA 224	ECDSA 256	ECDSA 384	ECDSA 512
Key generator (sec)	0.0151	0.155	0.219	0.303	0.621	1.573

Chapter 5: Simulation and Experiential result

In our research we compered two asymmetric algorithms RSA and ECDSA and we proposed the best one which is ECDSA for Information Centric network. For our experimental result we used 2,6 GHz Intel corie 5 machine with open SSL library and matlab simulator.

We Compered RSA with the key length of 512,1024,2048,and 4096 and ECDSA with the key length of 160,192,224,265,348 and 512 required time for signing and verifying of data packet and generating of public/private keys.

RSA Simulation Result

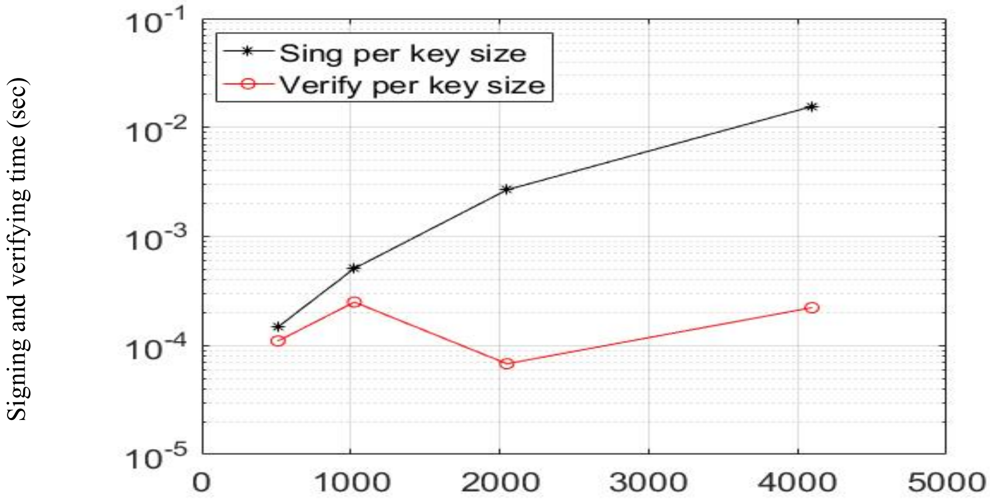

Figure1-5: Simulation result of time for RSA with key length 512,1024,2048,4096

Figure (5) Shows the RSA signing and verifying process in the figure Y-axis shows the verifying and singing time and X shows the key length as the key length is getting longer the verifying and singing process takes more time.

RSA Simulation Result

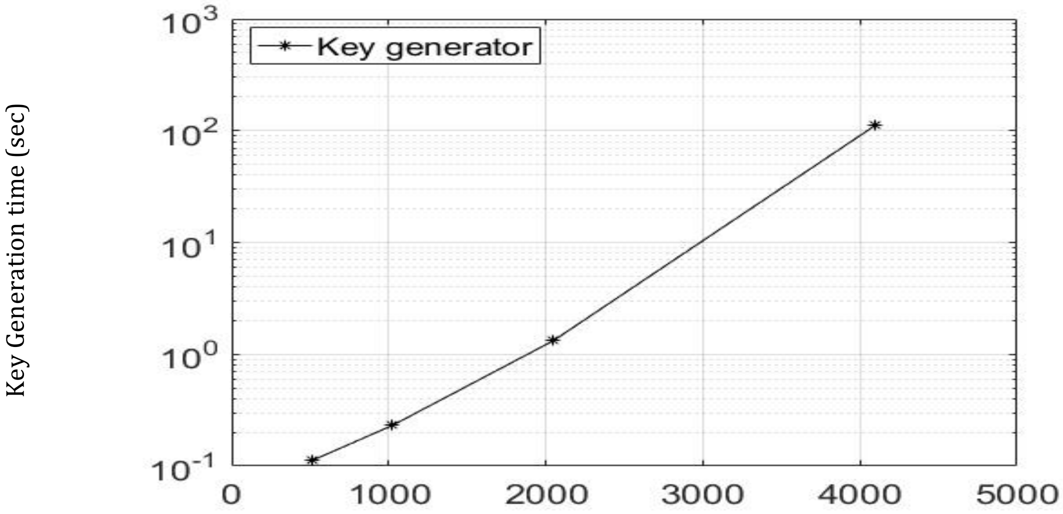

Figure 2.5: Simulation result of time of time for RSA with key length 512,1024,2048,4096

Figure(6) shows the public and private key generation time for RSA. X-axis shows the key length and Y-axis shows the key generation time, as the key is getting longer the key generation process is getting slow.

ECDSA Simulation Result

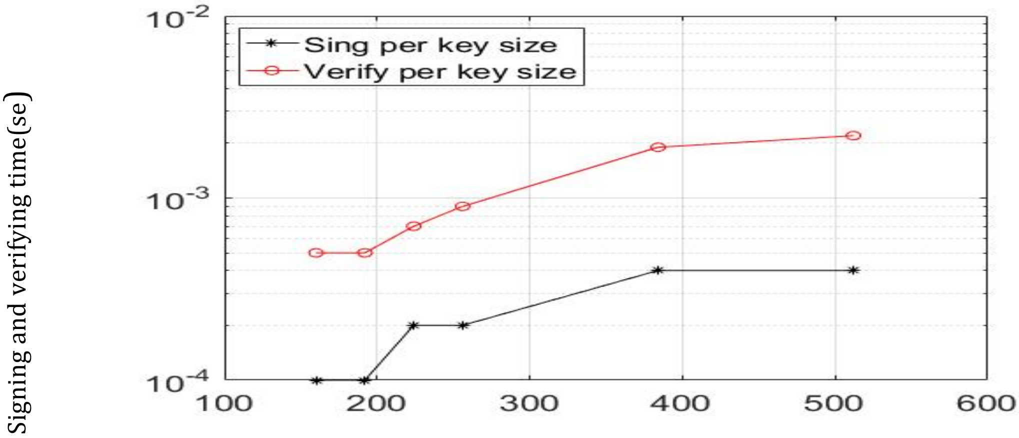

Figure 3.5 : Simulation result of time for ECDSA with key length 160,192,224,256,348 and 512 for singing and verifying

Figure(3) shows the signing and verifying process. X-axis shows the key length, and Y-axis shows the singing and verifying process. Our simulation result represents that he ECDSA verifying and signing process with smaller key size is faster than RSA with larger key size in Figure (1).

ECDSA Simulation Result

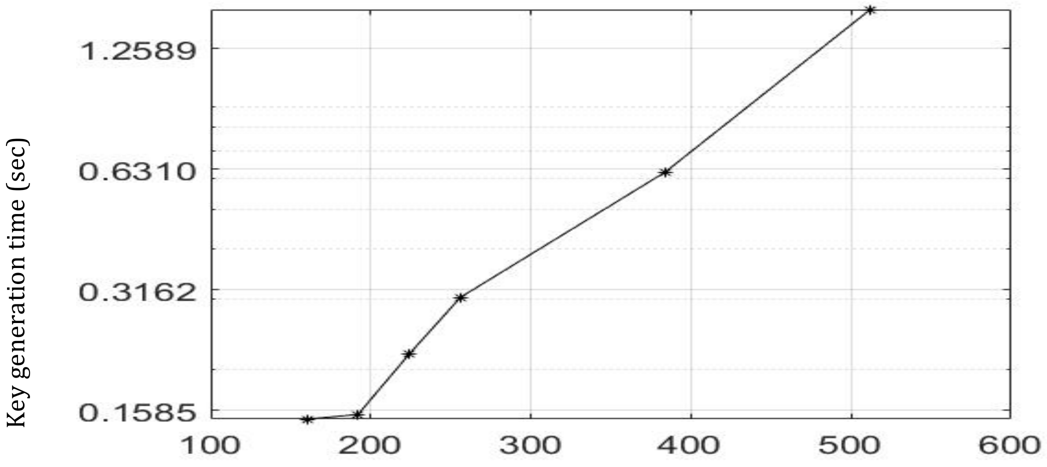

Figure 4.5:Simulation result of time for ECDSA with key length 160,192,224,265,348 and 512 for key generation.

Figure (4) shows the key generation time for ECDSA. Y-axis represents the ECDSA public and private key generation time and X-axis represents the key length of ECDSA our simulation result shows that with smaller key size ECDSA key generation is much faster than RSA key generation on figure2.

Chapter 6: Conclusion and Discussion

6-1:Elliptic Curve Digital Signature Algorithm Efficient Encryption and Decryption Algorithm Over Information Centric Networking

ECDSA algorithm is Asymmetric key cryptography which consist of two keys one public key and another one private key, Asymmetric encryption is more secure than symmetric encryption which use one key for encryption and decryption of cipher text and plain text for example AES (Advanced Encryption Standard) is symmetric encryption logarithm which is called secret key also. The main problem with AES is key exchange because in symmetric encryption the secret key has to be sheared, and each time when a new user added to the system the key should be share, in this cause the possibility of failing the key in the wrong hand is very high but in contrast Asymmetric algorithm uses two keys one is public key and another one is private key, public keys are published widely and private keys depend only to the owner.Two famous Asymmetric algorithms is RSA (Ronald Rivest,Adi Shamir, Lenorard Adleman) and ECDSA (Elliptic Curve Digital Signature), which uses for data encryption and digital signature. RSA has larger key size in comparison to ECDSA.RSA key lengths are 512,1024,2048 and 4096 bits. RSA security depends on large number factorization. From one side large keys length provides more security but from the other side it takes more time for Encryption and decryption and it is very slow which causes more processing power for both encryption and decryption. While ECDSA with smaller key size is much faster than RSA in terms of encryption and decryption. ECDSA keys length are160, 192,224,265,384 and 521 bits. ECDSA security is based on Elliptic Curve Desecrate Logarithmic problem. 192-bit

ECDSA key size has the equivalent security level to 1024 bit RSA key. In our work we compared the speed performance of RSA and ECDSA required time for singing and verifying of data packet and the required time to generate the private and public key. Our exponential result also shows that ECDSA is faster than RSA.

6-2: Conclusion

We proposed ECDSA algorithm for Information Centric Networking because one of the important factor for encryption and decryption is the time during process of encryption and decryption. ECDSA algorithm is faster and based on elliptic curve discrete Logarithm problem, which is the most secure digital signature scheme.

6-2:Future work

It is obvious that with the growth of Internet exchange of Audio, Video, text and image files also raised especially video traffic continues to grow on the Internet. Based on forecast video will make up nearly 80% of Internet traffic by the year 2020. M2M connection are calculated to grow nearly from 4.9 billion in 2015 to 12.2 billion by the year 2020,based on IOT forecast connected things will reach to 13.5 billion in the year 2020,from the all information about we arranged our future work which is compression, encryption and decryption of video, audio, text and image file based on ECDSA (Elliptic Curve Digital Signature Algorithm).

Because ECDSA has smaller key size, faster computation time that cause reduction in processing power, storage space bandwidth and from the other side ECDSA have ability of running on smaller devices or more compact software this also means less heat production and less power consumption.

Reference:

[1]Byung-keun-kim, Internationalizing the Internet the Co-evolution of Influence and Technology, year 2005,ISBN 1845426754, pages: 51-55

[2]Md Fazul Bari,Shihure Rahman Chowdhury, and Reza Ahmed, A survey of naming and routing in information –centric networks. IEEE Communications Magazine Year: 2012, Volume: 50, Issue: 12, DOI: 10.1109/MCOM.2012.6384450, Pages: 44 - 53

[3]Geouge Xylomenos,Christopher N .Ververidis,Vasilios George,Vasilios A.Siris,Nikos Fotiou,Christos Tsilopoulos, Xenofon Vasilakos,Konstations V. Katsaros,George C.Polyzos, A survey of Information-Centric-Networking Research, IEEE commuicaiton surverys & Tutorial 19 July 2014,volume16,Issue 2 , page 1024 - 1049

[4]JacobsonDiana K.SmeeersJames D.ThorntonMichael ,f.PlassNichols, H.Briggs,Rebeca L.Braynard,Networking Named content,proceeding of 5th international conference on emerging network conference on emerging networking experiments and technologies,Rome , Italy, December 01 - 04, 2009 ,01/4/2009 pages: 1-12

[5].Chris Chambers,Justin dolske, JayaRaman Iyer ,

From http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html

[6]Syed Hassan Ahmed, Safdar Hussain Bouk, Dongkyun Kim ,Content Centric Networks , An overview Application and Research Challenges ISSN 2191-8112 ,DOI 10.1007/978-981-10-0066-9, year 2016,pages 20-36.

[7]Eskan G.k Abduallah, Hassanein ,Mohammad Zulkernin ,survey of security attack in information centric networking ,IEEE Communication Survey & Tutorials.vol 17,No 3 Third quarter2015, Pages: 1024 – 1049

[8]Chirstof paarJan pelzl, Understating Cryptography,IABN 978-3-642-04100-6,DOI

[9]1007/978-3-642-04101-3 @springer-Verlag Berline Heidelberg 2010.

[10]Joan Daemen,Vincent Rijm,The design of Rjindeal,AES the advanced Encryption standard" . Springer, 2002 .ISBN 3-540-42580-2.

[11].Joselin.J ,S.J Brintha,V.Magesh Babu, Role of Digital Signature in Network Security and Cryptography. International Journal of Computer Science and Information Technologies, Vol.6 (1), 2015,pages: 893-895

[12] Aqeel Khalique , Kuldip singh,Sandeep Sood, Implementation of Elliptic Curve Digital Signature Algorithm ,International Journal of Computer Applications(0975-8887)Volume 2-No.2, May 2010,pages:21-27

[13]Xin Zhou , Xiaofei Tang .Resarch and Implementation of RSAR Algorithm for Encryption and Decryption.2011 the 6th International Forum on Strategic Technology .DOA:10.1109/IFOST.2011.6021216 page1118-1121

[14]Don Johson ,Alfred Menezes , The Elliptic Curve Digital Signature Algorithm

February 24 , 2000 , from :http:// www. Cacr.math.unwaterloos.ca

[15]Shweta Labma, Monika Sharma, An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA),21-23 Dec.2013 DOI:10.119/icmira.2013,pages:179-183