BIJIT - BVICAM's International Journal of Information Technology
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

Certificate Based Security Services in Adhoc Sensor Network

Shahin Fatima[1], **Shish Ahmad**[2] and **P. M. Khan**[3]

Submitted in June, 2014; Accepted in September, 2014

Abstract - The paper entitled "CERTIFICATE BASED SECURITY SERVICES IN ADHOC SENSOR NETWORK" proposed an approach in which the aim is to find the method for authentication which is more energy efficient and reduces the transmission time of the network. MANETs are of dynamic topology and have no predefined infrastructure. Due to its dynamic topology this network is prone to various kinds of vulnerable attacks. Sensor networks are battery operated and is a major concern. Methods on ID based Authentication consumes more network bandwidth and increases the computation and transmission time of the network. So for better operation, authentication must be the major factor of concern. In this paper a method for authentication in adhoc sensor network is proposed which is based on certificate based security services. Here we will make use of X.509 certificate format. In this some modification is made to the certificate format such that the transmission time and energy consumption of the network is reduced. Our proposed model will provide authentication among nodes and security in MANET. The proposed work is implemented in MATLAB and the result will show the effectiveness of proposed certificate in MANET. The objective of certificate based authentication is to ensure that messages can be read by authorized person only. It also overcomes the non repudiation attacks thereby minimizing the computation and shows how energy varies by making changes in certificate of node.

Index Terms – X.509 certificate, certificate authority (CA), authentication, confidentiality, securityHashing algorithm SHA-1, PrCA - Private Key of Certification Authority (CA), PuCA - Public Key of Certification Authority (CA).

1.0 INTRODUCTION

With the advancement in technology the need for wireless communication has also increased. As we know wireless communication can reach eventually on every surface of the earth and to millions of people. One of the kind of network is MANET (Mobile Adhoc Network) in which nodes does not have any predefined infrastructure [1]. This contrast to cellular network in which BS (base station) act as access point. MANET consists of a group of nodes that communicate with each other without having any predefined infrastructure. For example it may be used in natural disasters such as earthquakes where fixed infrastructures have got damaged & in such cases. A MANET is an autonomous system of mobile nodes [7] and can be used as a communication network for a rescue team in case of emergency. In MANET network topology may dynamically change and nodes are free to move. Security means physical protection of system by using appropriate policies and cryptographic techniques.

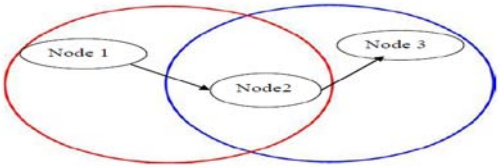


Figure 1: Example of Mobile Adhoc Network

As we can see in the figure it has three nodes, node 1, node 2 and node 3. Node 1 and node 3 are not within each other's range; hence node 2 can act as router to forward the packets from node 1 to node 2. Because we know that adhoc network are deployed randomly over a particular area so security here is a bit less important than security in various web services. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication [14]. In Adhoc network physical protection of device is very important and is a great challenge. Therefore, we depend and rely on cryptographic techniques for prevention of attacks. While designing security methods for mobile ad hoc networks, consideration about the attacks variations and the characteristics of the attacks should be kept in mind that could be launched against the ad hoc networks [8].

1.1 Need for security

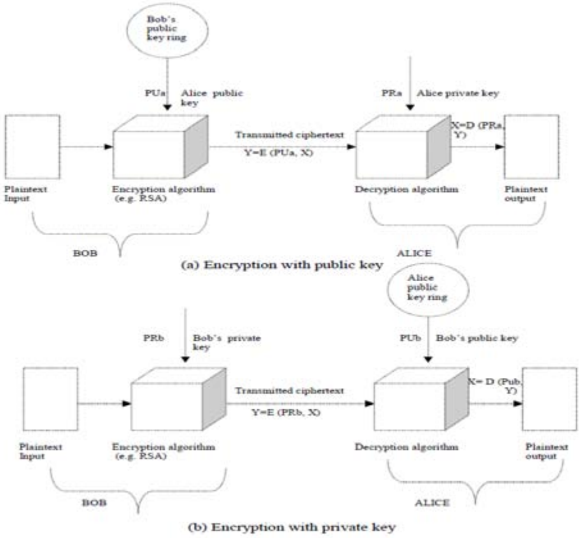
MANET's are practical and cost effective way for deployment of sensor networks. MANET's are used in large range of applications from civilian to military purposes. It throws different challenges as compared to traditional networks. Therefore different mechanisms can be brought about enormous research potential.

2.0 PUBLIC KEY ENCRYPTION

Asymmetric algorithm uses one key for encryption and same key for decryption. Symmetric encryption is vulnerable to brute force attack. To overcome from brute force attack the key size must be large enough. But because of large sizes the encryption & decryption speeds become too slow. Another way to attack is to find way to compute private key from the given public key. The history of cryptanalysis states that problems which seems to be insolvable can find a solution if looked from different way. Suppose for instance the message is to be sent & consist of 56 bit key. The attacker can encrypt all 56 bit key using public key & discover the encrypted key by matching the transmitted cipher text. Modern cryptography is basically designed for use on computers and no longer concerns about

[1, 2, 3] *Department of Computer Science and Engineering, Integral University, Lucknow*
EMail:[1]*shahinfatima@hotmail.com,*[2]*shish@iul.ac.in and* [3]*pmkhan@hotmail.com*

the written alphabet. Its focus is on the use of binary bits [10]. One of the main parts of the modern cryptosystem is quantum cryptography.



(a) Encryption with public key

(b) Encryption with private key

Figure 2: Public Key Cryptography

2.1 X.509 Authentication Service

X. 509 is a framework for authentication services .It uses Public-key Cryptography & defines authentication protocols. Certification authority signs the public key of user & stores the certificate in directory.

2.2 X. 509 Certificate Format

It is issued by certification authority CA & contains following fields:-
version which can be (1, 2, or 3)
serial number which is used for identification of certificate
signature algorithm identifier
issuer X.500 name i.e. name of CA
period of validity (from - to dates)
subject X.500 name (name of owner)
subject public-key info (algorithm, parameters, key)
issuer unique identifier
subject unique identifier

2.3 Need for X 509 Certificates

The X. 509 Certificate is needed because of following reasons:-

- X. 509 is more secure than using normal user ID or password
- It has trusted third party certifying authority which authenticates and distributes the digital certificates, thereby establishing a chain of trust.
- X. 509 also takes care of non repudiation attacks (i.e., the act of denying an action after the fact). For example, once someone uses a digital certificate and private key, the user cannot deny his action, because the private key resides with the user only.
- In X. 509 non authorised users face difficulty to extract the private key when stored on a smart card.

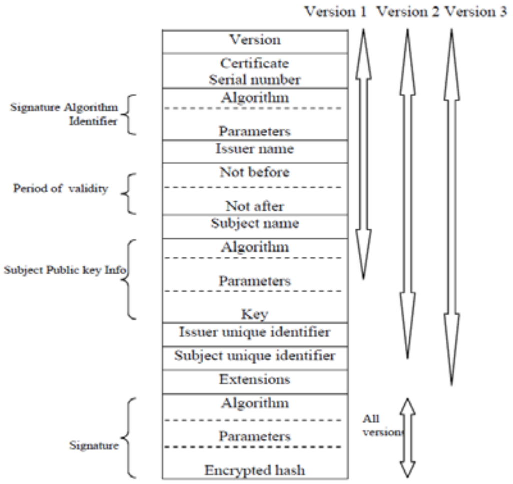


Figure 3: Format of X. 509 Certificates

2.4 Hashing Algorithm (SHA-1)

It is a cryptographic algorithm which is used to provide authentication & integrity of data. It is also used to avoid the need for storage of plaintext password in password based system. It is a function which takes input as block of data & returns the hash value in the form of fixed size string. It has the properties of primary resistance, second primary resistance and collision resistance. Hash Key management has been proposed as one of the best options for security, [9] although other options are also available depending upon need of security.

2.5 Encryption Algorithm (RSA)

This algorithm is based on factorising large prime numbers. This works on public & private key system. The public key is available to everyone [5]. This public key is used to encrypt the data. The decryption is done with the help of private key. This private key is associated with the user who will decrypt the message. The generation of private key from public key is very difficult therefore RSA algorithm is very popular for data encryption.

3.0 RELATED WORK

A mobile ad hoc network (MANET) consists of number of mobile stations connected by wireless links. It is known as infrastructure less network as it does not trust on predefined infrastructure. In MANET nodes can easily exchange information with nodes in its range and nodes which are beyond its range uses the concept of multihop communication.

Here we will study various national and international journals about the X 509 certificate and the proposed work for it in mobile ad-hoc network. There are various research papers related to this work & about the quality of X. 509. The research area related to this field is very broad. Following are few important research papers that describe the quality of X. 509. Mr. Vinod Saroha, Annu Malik, Madhu Pahal presents a survey on Digital Signature Certificate [2] which states about the digital signature, creation of digital signature, revocation of digital signature & authentication procedures. Digital signature ensures the identity of sender. A digital signature adds data electronically to any message in order to make it more authentic & more secured. Digital signature guarantees that once document is digitally signed then data cannot be tampered. Digital signature ensures security of message. The use of digital signature is to ensure that a user who is sending a message is the one who he/she claims to be.

Christian Bauer proposed an article "X.509 Identity Certificates with Local Verification" [3] which states that X. 509 identity certificate ensures authentication in communication system. A global trust anchor verifies this certificate which is accepted by communicating parties in order to authenticate each other. Because of non availability of services like certificate revocation services prevents proper authentication. In this paper X. 509 identity certificate is extended that allows authenticating parties to verify each other certificate in absence of global trust anchor. They have used this for describing their problem & giving the proposed solution. This paper states that revocation of certificate can be performed by using revocation service provided by trust anchor. M. Rameshkumar proposed "Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks" [4] which states that WSN can use μTESLA and MULTILEVEL μTESLA symmetric method for encryption. μTESLA methods have drawback that they suffer from DoS attacks. Therefore to overcome the weakness of μTESLA this paper presents key based method to achieve authentication. To overcome from the computation cost of these schemes, techniques such as hash tree & identity based schemes have been adopted. They have used one way hash function h () and uses the hash pre images as keys in a message authentication code (MAC). Dilbag Singh anf Ajit Singh proposed [14] A Secure Private Key Encryption Technique for Data Security in Modern Cryptosystem. They have proposed private key encryption technique which can be used for security of data in encryption. This technique employs the concept of arithmetic coding and can be used in any encryption system. This reference motivated me to apply a form of public key cryptography in my work for security and authentication.

4.0 PROPOSED WORK

The characteristics of MANET such as dynamic topology & energy constrained operation are a challenging issue. Security is also an important issue in the field of MANET. Security leads to authentication among nodes. Many methods have been proposed to provide security & authentication among nodes in MANET. In our work we will make use of X.509 authentication certificate format. We will modify the certificate format such that the size of certificate is reduced thereby leading to reduction in transmission time & energy consumption. This system will make use of RSA algorithm for encryption and SHA-1 logic for hashing

4.1 Proposed Certificate (X. 509 M)

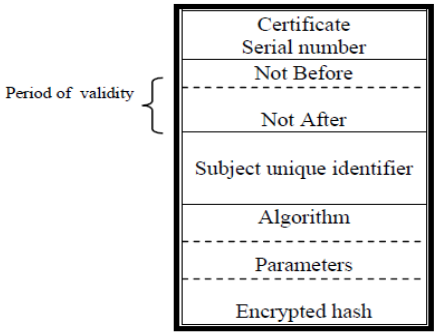


Figure 4: The (X.509 M) Certificate

In our proposed certificate the fields which are taken are as follows:-

- **Serial number:** It is an integer value unique within the issuing CA that is associated with the certificate.
- **Period of validity:** It consists of two dates: the first and last date on which the certificate said to be valid.
- **Subject unique identifier:** It is a bit string field which optional and is used to identify uniquely the subject.
- **Signature:** It covers all the fields of the proposed certificate. It also contains the hash value of all the other fields and encrypted with the CA (Certification Authority) private key. This field includes the signature algorithm identifier.

4.2 Security Model for MANET

The security model for MANET consists of encryption and decryption of signature among nodes in MANET.

4.2.1 Encryption and sending signed message to Y

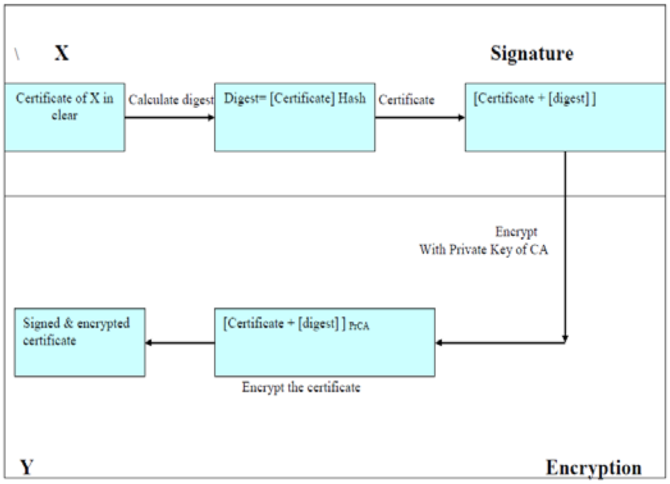

\ X
Signature
Certificate of X in clear
Calculate digest
Digest= [Certificate] Hash
Certificate
[Certificate + [digest]]
Encrypt
With Private Key of CA
Signed & encrypted certificate
[Certificate + [digest]] PrCA
Encrypt the certificate
Y
Encryption

Figure 5: Signature and Encryption details with signature & key

Figure shows the operation required when X wants to send a signed & encrypted certificate to Y.
It consists of following steps:-

4.2.1.1 Certificate Signature

The signature includes two steps:-

- **Message Digest Evaluation**
  This is called as hashing. The main purpose for calculating digest is to ensure that message is unaltered & ensuring message integrity
- **Digest Signature**
  The signature is calculated by encrypting it with CA's private key. The hashing algorithm is also included in the signature. By using public key encryption & hashing algorithm the recipient has the proof that:
    - The CA's private key has also encrypted the digest
    - The message is not modified against any alteration.

4.2.1.2 Message encryption

Encryption includes 3 steps:-

- **Creating encryption/decryption key**

Here we will create key for one time for encryption/decryption algorithm which is public and private key of CA.

- **Message encryption**

The whole message is encrypted with private key of CA.

- **Key used for Encryption**

Public key of CA is the key used by the receiver side to decrypt the message. Therefore public key of CA must be available to recipient only.

4.2.2 Decryption & Verification of signature of message

Figure shows the steps required when Y wants to decrypt & verify the message send by X.

4.2.2.1 Message decryption

This involves the following steps:-

- **Message decryption**
  The certificate is now decrypted using public key of CA. The one time public key of CA is used to decrypt the message.

4.2.2.2 Signature Verification

It includes the following steps as follows:-

- **Message digest decryption**
  The digest was encrypted using CA's private key. This can now be decrypted using CA's public key.
- **Digest Evaluation**
  Because hashing is only a one way process therefore the original message cannot be derived from certificate, the recipient has to calculate the hash again using the similar hashing algorithm as used by the sender.

- **Comparison of digest**
  The digest which got decrypted above & the digest evaluated above will be now compared. If both get match then the signature is said to be verified & recipient can accept the messages coming from the issuer.

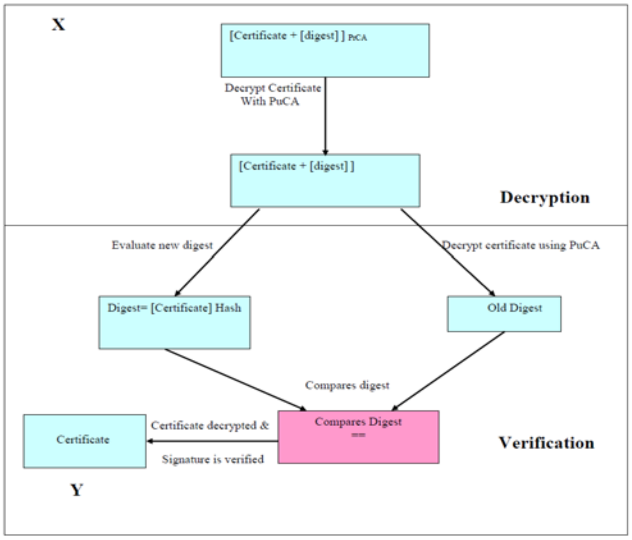


Figure 6: Signature & Decryption details with certificate and keys

If a mismatch occurs then it means that:-

- The message is not signed by CA's private key
- The message is altered
- In both the above cases the message should get rejected.

5.0 RESULTS AND DISCUSSION

Here we will evaluate our model Certificate based security services in Adhoc Sensor Network. The parameters used for simulation will be compared to the existing certificate. It is very important to choose suitable parameters for system evaluation. The performance parameters will describe the result of simulation. These parameters are important as they will be used to notify what will actually happen during simulation. MatLab- 2010 will be used as simulation tool because Matlab uses the hierarchal architecture in order to define components like nodes & network.

The experiments were carried out by MatLab-2010. The scenarios developed to carry out the tests use as parameters the mobility of the nodes and the number of active connections in the network. Node are presented previously	Matlab-2010

were utilized in the experiments. The choices of the simulator are presented in table 1	
Simulation Area	100*100m
No of nodes	10 to 100
Transmission range	25m
Mobility Model	Random Waypoint
Max Speed	5-20 m/sec
Traffic Type	CBR(UDP)
Data payload	1500 bytes
Packet rate	2 packet/sec
Sensor type	Crossbow MICA2DOT mote.
Simulation time	30 sec
MAC	802.11
Pause Time	20 sec
Mobility	10.70 m/s
Terrain area	100*100m

Table 1: Measurement of MATLAB

5.1 Validation in terms of metrics used for comparison

In this section we will validate our thesis by comparing modified & original certificate based on various parameters. The sensor used for validation is Chipcon CC1000 radio in Crossbow MICA2DOT mote.

5.1.1 Energy Consumption in transmission & reception

$E_s = (E_{tx})$

$E_r = (E_{rx)}$

Where,

E_{tx}–It is the energy required to transmit a byte.

E_{rx}–It is the energy required to receive a byte.

Here we will calculate the energy consumption due to transmission/reception of varying certificate sizes.

The energy consumption in transmission of 1 byte is 28.6 µJ [4] respectively. The energy consumption in reception of 1 byte is 59.2 µJ [4] respectively. For proposed certificate the size is of 31 bytes, therefore total energy associated with proposed certificate in transmission is 886.6 µJ and 1835.2 µJ in reception respectively.

The original size of X.509 certificate is of 82 bytes; therefore total energy associated with proposed certificate in transmission is 2345.2µJ and 4854.4µJ in reception respectively.

5.1.2 Energy consumption on computation

Here we will calculate the computation overhead of the proposed schemes in terms of energy consumption. The energy consumption in 1 byte of computation is 7.6mJ respectively [4]. For proposed certificate the size of 31 bytes requires energy consumption as 235.6 mJ.

The original size of X.509 certificate is of 82 bytes; therefore total energy associated with proposed certificate is 623.2 mJ.

5.3.4 Transmission time

It is the amount of time from beginning till the end of message transmission. The cost of 1 byte in transmission is $8.8*10^{-4}$ msec [6] respectively. Therefore the transmission cost associated with total size of proposed certificate is $2.728*10^{-2}$ msec.

The cost associated with 82 bytes of original certificate is $7.216*10^{-2}$ msec.

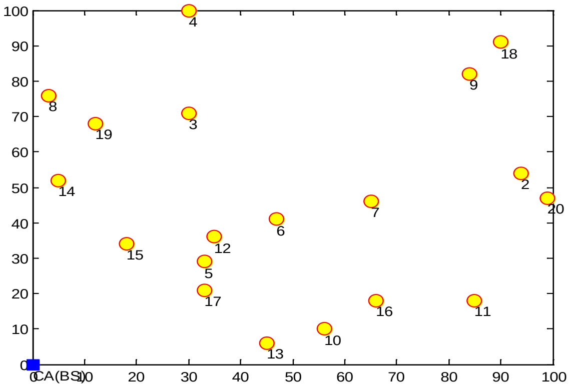


Figure 7: Displaying no of nodes in 100*100 area with CA

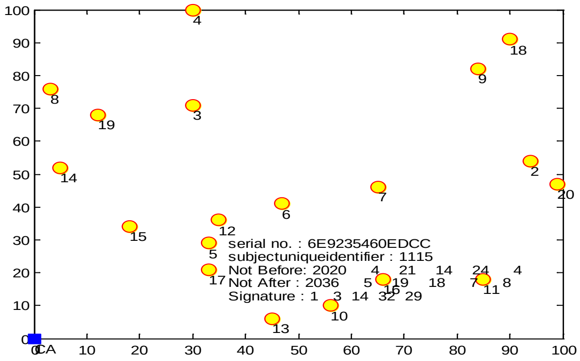


Figure 8: Displaying certificate of a specified nodes

7.0 CONCLUSION & FUTURE WORK

Security is an important issue for communication among nodes in Mobile Adhoc Network because of its important characteristics like infrastructure less and dynamic topology. By using X. 509 certificate we can provide better security & authentication among nodes in network. With the help of X. 509 certificates the network can be protected against unauthorized access. The advanced technology in adhoc network is facing issues related to proper key management. The security of MANET is coping up from these issues to provide better security. MANET consists of mobile nodes and because of its dynamic nature it faces many challenges. Our proposed model will provide authentication among nodes and security in MANET. The proposed work is implemented in MATLAB and the result will show the effectiveness of proposed certificate in MANET. The proposed work will initially reduce the size of original certificate which is then deployed among nodes in MANET by CA (Certification Authority). The proposed solution shows a great improvement over X.509 certificate in terms of computational energy, transmission/reception energy and transmission time.

The future scope of work is that the proposed authentication scheme of modified X.509 certificate can be used in MANET by forming clusters among nodes in MANET. Each cluster will have cluster head CH which will act as certification authority CA. This CA will a lot the certificate to its child nodes and keep the record of malicious nodes & original nodes in its respective cluster. This will improve the security among nodes in MANET. This technique can also be used on mobile Certification Authority (BS). The tedious task will be then how to select CA.

8.0 ACKNOWLEDGEMENT

I would like to thank the institution who helped a lot in this study. Also, special thanks to my guide and co-guide in sparing their time providing their valuable inputs as and when required during the course . Many thanks to all the peers, colleagues and organizations who supported this research by sharing their valuable time and feedback on their experiences in application of X.509 Authentication Certificate in Adhoc Sensor Network.

9.0 REFERENCES

[1]. Carloss De Morais "Adhoc & Sensor Network ", ISBN- 981-256-681-3 Pg [1] [2].

[2]. Mr. Vinod Saroha, Annu Malik, Madhu Pahal : The Enormous Certificate: Digital Signature Certificate International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013 ISSN: 2277 128X

[3]. Christian Bauer: X.509 Identity Certificates With Local Verification First IEEE International Workshop on Security and Forensics in Communication Systems Institute of Communications and Navigation, German Aerospace Center (DLR), Wessling, Germany.

[4]. M.Rameshkumar ,"Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks" Volume 2, Issue 10, October 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[5]. William Stallings "Cryptography and network security principles and practice fifth edition", ISBN- 10: 0-13-609704-9 Pg [428].

[6]. Thomas Kunz, S.S.Ravi: Ad-hoc Mobile and Wireless Network: 5th International Conference on Adhoc Sensor Network, ISSN-0302-9743 Pg [174].

[7]. Ashema Hasti, "Study of Impact of Mobile Ad – Hoc Networking and its Future Applications" in BIJIT January - June, 2012; Vol. 4 No. 1; ISSN 0973 – 5658 439

[8]. B. B. Jayasingh1 and B. Swathi, "A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network" BIJIT – 2010; Jan – June, 2010; Vol. 2 No. 1; ISSN 0973 – 5658

[9]. Ashwani Kush1 and C. Hwang, "Hash Security for Ad hoc Routing", BIJIT – 2011; January – June, 2011; Vol. 3 No. 1; ISSN 0973 – 5658

[10]. Dilbag Singh1 and Alit Singh, "An Effective Technique for Data Security in Modern Cryptosystem", BIJIT – 2010; Jan – June, 2010; Vol. 2 No. 1; ISSN 0973 – 5658

[11]. National Institute of Standrads and Technology. Recomended elliptic curves for federal government use, 1997.

[12]. Albert Levi and Erkay Savas. Performance evaluation of public-key cryptosystem operations in WTLS protocol. In (ISCC'03), pages 1245–1250. IEEE Computer Society, 2003.

[13]. Richard Kuhn, Vincent Hu, Timothy Polk, and Shu-Jen Chang. Introduction to public key technology and the federal PKI infrastructure. NIST, February 2001.

[14]. Dilbag Singh and Ajit Singh "A Secure Private Key Encryption Technique for Data Security in Modern Cryptosystem" in BIJIT Issue 4: (July-December, 2010 Vol 2 No 2).

certificate for node 1 serial no. : 6E9235460EDC8 subjectuniqueidentifier : 1111 Not Before: 2019 6 6 12 9 4 Not After : 2037 7 28 17 35 49 Signature : 1 3 14 32 29	**certificate for node 2** serial no. : 6E9235460EDCE subjectuniqueidentifier : 1112 Not Before: 2021 12 1 21 37 60 Not After : 2032 6 25 6 30 55 Signature : 1 3 14 32 29
certificate for node 3 serial no. : 6E9235460EDC7 subjectuniqueidentifier : 1113 Not Before: 2018 11 23 15 15 40 Not After : 2020 8 20 18 54 59 Signature : 1 3 14 32 29	**certificate for node 4** serial no. : 6E9235460EDCC subjectuniqueidentifier : 1114 Not Before: 2020 7 28 14 2 8 Not After : 2038 6 26 6 34 38 Signature : 1 3 14 32 29
certificate for node 5 serial no. : 6E9235460EDBC subjectuniqueidentifier : 1115 Not Before: 2013 8 11 2 30 12 Not After : 2016 3 5 5 3 39	**certificate for node 6** serial no. : 6E9235460EDC2 subjectuniqueidentifier : 1116 Not Before: 2015 7 21 12 33 27 Not After : 2018 6 26 21 17 13

Signature : 1 3 14 32 29	Signature : 1 3 14 32 29
certificate for node 7 serial no. : 6E9235460EDC6 subjectuniqueidentifier : 1117 Not Before: 2018 8 13 5 57 5 Not After : 2021 2 5 15 35 4 Signature : 1 3 14 32 29	**certificate for node 8** serial no. : 6E9235460EDCF subjectuniqueidentifier : 1118 Not Before: 2022 9 23 2 52 57 Not After : 2042 11 24 13 11 24 Signature : 1 3 14 32 29
certificate for node 9 serial no. : 6E9235460EDBE subjectuniqueidentifier : 1119 Not Before: 2014 1 29 8 18 20 Not After : 2024 8 1 21 34 52 Signature : 1 3 14 32 29	**certificate for node 10** serial no. : 6E9235460EDC4 subjectuniqueidentifier : 1120 Not Before: 2016 6 2 5 40 20 Not After : 2034 2 30 13 43 60 Signature : 1 3 14 32 2

Table2: showing certificates of 10 nodes

hash code of node(1): hash coding time 0.7500 02AEF106 A9697608 1AFF4891 804B1BD3 906F0597	Intaializing: RSA encrpted certiicate : 75 84 109 137 42 26 75 10 109 63 10 63 132 10 75 23 26 109 42 42 171 23 63 26 23 75 171 77 26 77 85 68 63 75 10 42 75 25 63 132
hash code of node(2): hash coding time 0.3290 FA8E33BF 86310A61 64684DA1 BE52379C 3A5D4D41	Intaializing: RSA encrpted certiicate : 42 109 23 137 68 68 77 42 23 10 68 26 75 109 10 26 10 171 10 23 171 85 109 26 77 137 25 84 68 132 63 67 68 109 25 85 171 85 171 26
hash code of node(3): hash coding time 0.3280 EC059560 D62BC9AA DF9F5D53 0245639C F2C2E118	Intaializing: RSA encrpted certiicate : 137 67 75 25 63 25 10 75 85 10 84 77 67 63 109 109 85 42 63 42 25 85 25 68 75 84 171 25 10 68 63 67 42 84 67 84 137 26 26 23
hash code of node(4): hash coding time 0.3130 669977FB 08751621 93A2E205 7736C27F B8D6489	Intaializing: RSA encrpted certiicate : 10 10 63 63 132 132 42 77 75 23 132 25 26 10 84 26 63 68 109 84 137 84 75 25 132 132 68 10 67 84 132 42 77 23 85 10 171 23 63 25

Table3: Calculated hash codes along with encryption at all nodes

Enter the no. of nodes that are willing to communicate any no. from 1 to20: **Enter no of first node:** **Enter no of second node:** **nodes 2 and 3 are selected to communicate**	Decrypted ASCII of Message: 137 67 75 25 63 25 10 75 85 10 84 77 67 63 109 109 85 42 63 42 25 85 25 68 75 84 171 25 10 68 63 67 42 84 67 84 137 26 26 23
Decrypted Hash Message is: EC059560 D62BC9AA DF9F5D53 0245639C F2C2E118	Hash code of node 3 after decryption :- EC059560 D62BC9AA DF9F5D53 0245639C F2C2E118
The hash code of selected node is similar before and after decryption, Hence Selected node is authentic to communicate	

Table 4: Decryption at receiver side & comparison of calculated hash

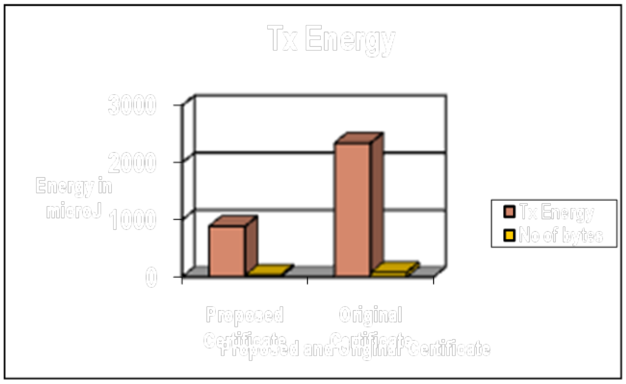


Figure 9: Transmission energy of proposed & original certificate

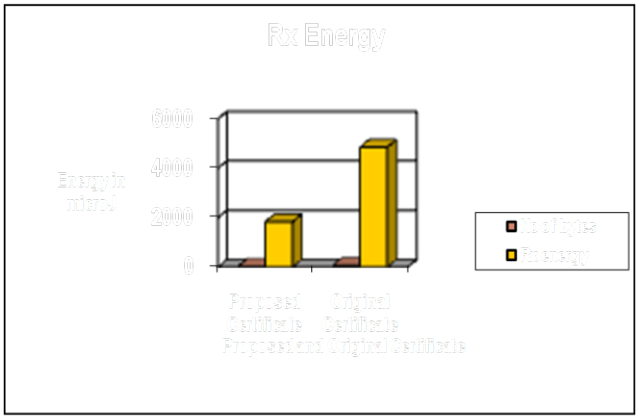


Figure 10: Reception energy of proposed & original certificate

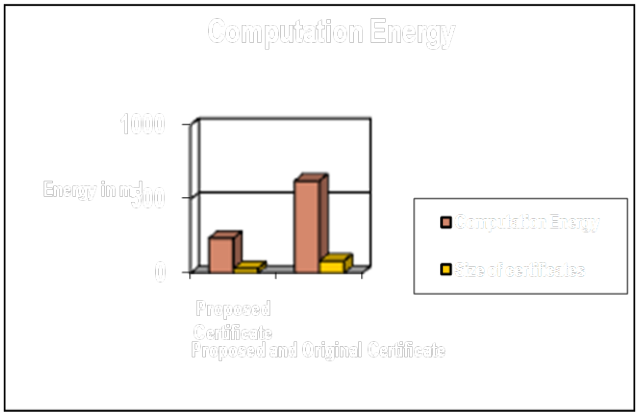


Figure 11: Computational energy of proposed & original certificate

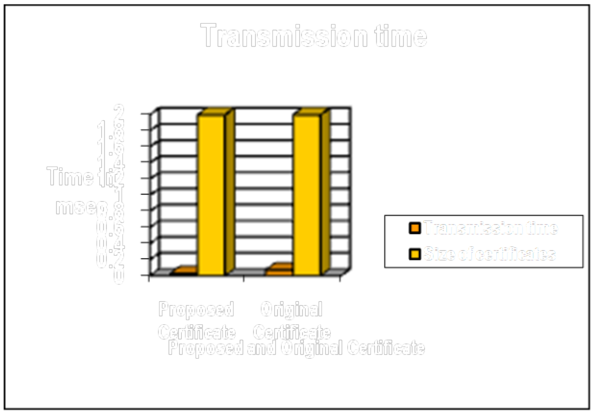


Figure 12: Transmission of proposed & original certificate

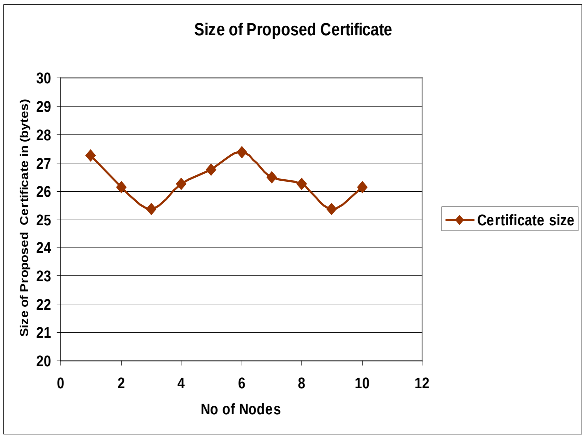


Figure 13: Size of proposed & original certificate with varying nodes.

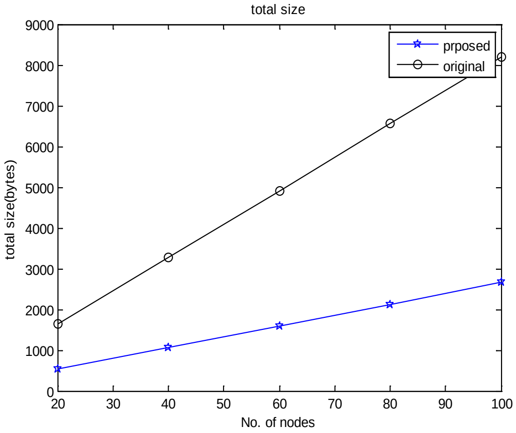


Figure 14: Size of proposed & original certificate with varying nodes.