International Journal of Pure and Applied Mathematics

Volume 119 No. 17 2018, 1279-1284

ISSN: 1314-3395 (on-line version)

url: http://www.acadpubl.eu/hub/

Special Issue http://www.acadpubl.eu/hub/

**A REVIEW PAPER ON CRYPTOGRAPHY AND NETWORK SECURITY**

*1Sujatha .K, , D.Ramya* Devi Kala Rathinam. D

1Assciate professor, , 2Assistant professor, 3PG Scholars

Dept. of Computer Science and Engineering

Sri Krishna College of Engineering and Technology, Coimbatore, India

117epcs004@skcet.ac.in

**ABSTRACT**

Cryptography and Network Security is used to protect network and data transmission takes place over

wireless network. Providing security to the data is one of the main aspect of data transmission over wireless unreliable network. The wireless networks consist of sensors; it is connected to base station. The security need for wireless sensor network is very essential and it is provided by cryptography and network security. The network security not only required to provide security to end system but also to the entire network system. Providing security to network is one of the important issues because the world is moving into digital world. Network security provide security to data which is controlled by administrator. The data should be accessed only by authorized user; this security is provided by network security. It takes place in all type of public and private network where transaction and data communication takes place. Some networks can be private it takes place within organization and some networks can be private. Compression is a process of reducing byte or bit to represent the data. Network security is used in various applications like government agencies, organization, enterprises, bank, business and also in some other applications. In Cryptography some algorithms are used to provide security to networks. In this paper we discussed about cryptographic principles, cryptosystem types and cryptographic model and its algorithm. It is about confidentiality, authentication and integrity during access of confidential data.

Keywords: Cryptography, Compression, Network security, Encryption, Decryption

**INTRODUCTION**

Network Security is responsible for providing security to all the information passed over the internet from

one computer to other. Network Security refers to all software and hardware functions, accountability [1], features, administrative and management, measures, characteristics[2], access control, information in a network and operational procedures are acceptable level to protect software and hardware. Cryptography is one of the emerging technology used for providing security to data. The authorized user should provide user ID and password or any other unique data to access secured data[3]. It used to keep the information more secure and safe. There are four network security problems: nonrepudiation, secrecy, confidentiality and authentication. Secrecy is a term used for keeping the data more confidential without accessed by unauthorized users. Authentication need to keep the data more sensitive. Nonrepudiation always deals with signature. Message Integrity used to ensure the secure connection between sender and receiver[4]. Cryptography is the process of writing in secret code. Cryptography has many applications like computer passwords, ATM cards, e-commerce, electronic commerce, business applications and also in some other applications. Cryptography is nothing which is closely related to cryptology and cryptanalysis. Two technologies are used in cryptography. Encryption used in sender side and the decryption is used in receiver side[5]. The decryption cannot perform without knowledge of encryption. Cryptanalysis is used for “breaking the code”. The area where we have both cryptanalysis and cryptography is called as cryptology. There are many powerful techniques but among them AES is one of the most powerful and useful techniques. Cryptography use many algorithms and some principles.

1279

International Journal of Pure and Applied Mathematics Special Issue

Fig 1: Crypto system

**LITERATURE SURVEY**

Prof. Mukund R. Joshi, Renuka Avinash Karkade proposed the paper on Network Security with Cryptography [6]

In this paper some principles of cryptography is discussed. The Redundancy and Freshness are two principles used in cryptography. The message should be encrypted at the sender side but all the encrypted message contain some redundancy. The freshness use timestamp to receive the message. The time is set for each message the received message is within the time limit the message is accepted. The message exceeds the time limit before receiving to receiver, those messages are discarded [7]. Two classes are used in cryptography, symmetric and asymmetric cryptographic algorithm. In symmetric cryptographic algorithm same key is used in both sender and receiver side. But in asymmetric cryptographic algorithm different key is used in sender and receiver side. In encryption the plain text is converted into cipher text. The decryption is reverse process of encryption, covert cipher text into plain text.

Cryptographic system provide privacy and authentication in communication system. Asymmetric cryptosystems use two types of keys one is public key and another one is private key [8]. The key distribution is suggested by Diffie and Hellman.

Shyam Nandan Kumar proposed Review on Network Security and Cryptography [9]

In this paper the types of Security Attacks are discussed. Active Attacks do some modification in data stream. The types of active attacks are Modification of Message, Denial of Service, Replay and Masquerade. Modification of Messages makes some changes or reorder the message format. Passive Attacks used for monitoring the communication. In Traffic Analysis attacks the message is read by third party. Release of Message Contents attacks the message read by sender and receiver. Some Security Services are provided for data transmission. Data Integrity, Data Confidentiality, Authenticity, Nonrepudiation and Access Control are some of the security services provided by cryptography.

Madhumita Panda proposed a paper on Security in Wireless Sensor Networks using Cryptographic Techniques

In this paper the Cryptography is used in Wireless Sensor Network to provide security to the wireless communication. Some security requirements are used in wireless sensor network like Confidentiality, Authentication, Integrity and Availability. Some obstacles of sensor security is used within a Very Limited Resources. The Very Limited Resources includes Limited Memory and Storage Space, Power Limitation and Transmission range. Unreliable Communication is also one of the obstacles Unreliable Transfer, Conflicts and Latency [10]. Unattended Operation is one of the obstacles like Exposure to Physical Attacks, Managed Remotely and Lack of Central Management Point. Symmetric key is also called as secrete key. It use only one key on both sender and receiver side. Asymmetric Cryptography is called as public-key cryptography. It use different keys on both sender and receiver side.

1280

International Journal of Pure and Applied Mathematics Special Issue

**CRYTOGRAPHIC PRINCIPLES**

**A. Redundancy**

Cryptographic principle 1: All the encrypted message contain some redundancy, there is no need of understanding the message by information.

**B. Freshness**

Cryptographic principle 2: Timestamp is used in every message. For instance the time stamp is of 10sec for every message. The receiver keeps the message around 10sec to receive the message and filter the output within that 10sec. The message exceeds the timestamp it is throw out.

Fig 2: Cryptography

**CRYPTOSYSTEM TYPES**

**Asymmetric cryptosystems**

It use two different keys to send and receive the messages. It use public key for encryption and another key is used for decryption. Two user A and B needs to communicate, A use public key of B’s to encrypt the message. B use private key to decipher the text. It is also called as public key cryptosystems. Diffie- Hellman key exchange generate both public and private key.

Fig 3: Asymmetric cryptosystems

**Symmetric cryptosystems**

In Symmetric cryptosystems both the enciphering and deciphering keys are identical or sometimes both are related to each other. Both the key should be kept more secure otherwise in future secure communication will not be possible. Keys should be more secure and it should be exchanged in a secure channel between two users. Data Encryption Standard (DES) is example of Symmetric cryptosystems.

1281

International Journal of Pure and Applied Mathematics Special Issue

Fig 4: Symmetric cryptosystems

**CRYPTOGRAPHIC MODEL**

**Encryption model**

In Encryption model the plain text is converted into cipher text. There are two types of keys are used in Encryption model. One is Symmetric key or private key and another one is public key. In Symmetric encryption only one key is used for communication. Plain text can be encrypted using some encryption algorithm.

**Decryption model**

In Decryption model the cipher text is converted into plain text using both Symmetric and Asymmetric decryption. In symmetric decryption single key is used for both encryption and decryption. In asymmetric key use two different keys for communication.

Fig 5: Cryptographic Model

**CONCLUSION**

Cryptography is one of the most important component to provide security to data communication between networks. It used to protect data from unauthorized users. The key is exchanged between sender and receiver should be done more in secure way. The key should be known only to sender and receiver otherwise security issue will gets arise. In this paper the cryptosystem with its model is discussed regarding the network security. The data can be compressed to reduce the cost for communication. The redundancy can be avoided after data compression it reduce

1282

International Journal of Pure and Applied Mathematics Special Issue

the storage space. There are two types of compression used in network security to compress the data. Lossy and Lossless methods are two compression methods. Some cryptographic algorithm are used in network security to provide the secured communication[11]. The exchange of key should be done more secure. Cryptography and network security is used in data communication over internet to provide the security.

**REFERENCE**

1. Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security* (pp. 36-54). Springer, Berlin, Heidelberg.

2. Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. *International Journal Of Engineering And Computer Science*, *6*(4).

3. Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. *arXiv preprint arXiv:1412.2495*.

4. Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. *Advances in Computational Sciences and Technology*, *10*(5), 763- 770.

5. Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. *American Journal of Engineering Research (AJER)*, *3*(01), 50-56.

6. Dhamdhere Shubhangi, T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

7. Kumar, S. N. (2015). Review on network security and cryptography. *International Transaction of Electrical and Computer Engineers System*, *3*(1), 1-11.

8. Kaur, S., Kaur, R., & Raina, C. K. (2017). Review on Network Security and Cryptography. 9. Duong, T., & Rizzo, J. (2011, May). Cryptography in the web: The case of cryptographic design flaws in asp. net. In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 481-489). IEEE. 10. Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India. 11. Krishnamoorthy, Dr, and S. Chidambaranathan. "Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs." (2017).

1283

1284