International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Survey on network based cryptographic techniques for key generation and data Encryption/Decryption

Digvijay Pawar[1]

[1]*PG Student, Dept. Of Information Science and Engineering, Acharya Institute of Technology, Karnataka, India*

Abstract - *Nowadays internet is growing with tremendous speed where the network threats and issues are increasing. Information security plays a vital role in providing data confidentiality, availability, integrity and security where the sender and receiver has to ensure secure transmission of data between source and destination nodes using encryption and decryption techniques. In the existing system, the security provided at the data link layer for large Ethernet networks using GKSP (Group based MAC key selection protocol). But this scheme has issues like security integration at network layer, efficient key sharing and node overhead etc. In this paper focuses on how data security will be carried out at Network layer with the help of Security functions like Encryption, Decryption and Key exchanging algorithms.*

Keywords: **Encryption/Decryption, NS2, Security at Network Layer , Key Sharing, , GKSP.**

1. INTRODUCTION

Security in the Internet world determines the power of the system to oversee, keep safe and make distribution sensitive information. Data Security was discovered many years before because everyone needs to send information without making open its content to others. The first and most certain machine was used in the second world war by the German military to encrypt their notes.

Network security is consists of the policies took up to prevent and monitor the denial of computer network ,modification, authorized access and misuse of secret information. The main purpose of network security is to keep safe (out of danger) the underlying networking 2 base structure from unauthorized access, misuse, modification, destruction, thereby making come into existence a secure flat structure Network security begins with authentication, which it provides using a username and a password. Another way to provide security is using firewall.

This paper gives a detailed account of security module where encryption, key sharing features as well as decryption features are developed in a NS-2. Mainly for wired network the new protocol is added at the network layer. For new security protocol a new packet format is defined. In NS2 new protocols are derived from built-in class. we add an encryption and decryption functions in derived class. This paper is also takes care of key sharing functions to make certain the secretly of data packet during sending and simulation implementation is carried out by NS2 simulator. NS 2 is an open source and it is designed using C++ and TCL(Tool command Language) language. The paper's structure is given as follows. In Part 2, deals on Related work, In Part 3 explanation on Encryption & Decryption techniques and finally the conclusion of s paper in Part 4.

2. RELATED WORK

Sourabh Chandra et.al[1]In this paper, the author has proposed few existing methods depends on Symmetric key cryptography mechanism it is science of keeping information safe and secret and they made a basic comparison work among them. . And also they have mentioned various Symmetric key cryptography which are using in real world few of them are- Introduction of chips and cards[1] it has some features like, it provides independent data get moved from one position to another and has different key management functions. The chip provides low hardware penalty with high fault treatment and provides an maximum output of more than 177 Mbps. The applications are trading, businesses like information for computers and making connections with hard disks, the national administrations and FDDI are high rate network protocols,. Another example is securing the information in the cloud[1] where the metadata server, a storage node and an application node which are belongs to a particular system. The Public clouds consists of Identity-based remote data property is having a cloud server and private key generator**.** The exchanging information and overhead calculation of a protocol is very low and applications are Cloud computing , mobile internet and so on. Symmetric key encryption algorithm depends on having an effect equal to the input geometry[1] it is a type of symmetric key encryption technique where as its features are in any unreliable communication both transposition and exchange methods are applied to a secret image, potentiality and strengths are considered for the safety needs of digital images. For both encrypted and secret images, the correlation value is one and its applications are Military systems, Medical and advertisement.

ShuminXu, YataoYang [2] Proposed a paper which gives describes of wireless network model is developed based on NS2 simulator. The network operations, such as , packet loss rate, system delay, throughput and other key elements are simulated. By running of tcp and UDP protocols, they make the observations and evaluations to network operations from different forms and then related parameters were graphically compared with gnuplot. Finally they have got positive referenced values in their simulation results .

JIANG Hong and et al.[3] They have discussed management schemes and secure key agreement based on IEEE 802.1af, It includes generation of keys, distribution of keys and detection of live peer lists. In this paper they have made comparison between LKS (LAN-based key server) and KSP (Key selection protocol). After these two protocols for large Ethernet networks the GKSP (Group based key selection protocol) is used to enhance the security of Ethernet. In LKS, election is carried out and based on that election key server is generated both Key management and distribution is depends on key server. Each MKA (MAC Security Key Agreement message) contains the status of a node and the key server is identified.

By that status information of each message. The election procedure is carried out under these following conditions:

1. No key server exists
2. Existing key server is non-responsive

For more than 100 nodes both LKS and KSP are have some drawbacks in large Ethernet networks. A GKSP (Group based MAC key selection protocol) is proposed to improve the efficiency of a key agreement.

Vojislav B., Jun Fung, and Jelena[4] They discusses security issues in IEEE 802.15.4 standard [4] i.e low-rate wireless personal area networks (LR-WPANs) . A number of issues are identified at Data link and Physical layer , and also in data link layer possible attacks are outlined, some of which can be directly launched.

Usually MAC layer attacks concentrate on distracting the channel which is used for regular access of nodes, thus it leads to distracting the data or information flow in sensor node, and it is responsible for DoS condition at link layer. Finally, physical layer (jamming) attacks where attackers sending the unwanted signals which distract the data flow through radio frequency interference. Jamming at the MAC layer is achieved by sending large size data packets with unwanted or unrelated information. In this paper, they have identified a numerous number of security issues in Physical layer and MAC layer but they only concentrate on IEEE std 802.15.4 i.e low-rate wireless personal area networks (LR-WPANs)

To simulate and analyze dynamic nature of communication networks, the Network simulator tool is used i.e NS2 [5] (second version of network simulator). Network simulator-2 is worldwide accepted and open source simulation tool, mainly to simulate new functions and protocols this powerful tool has been used. NS2 supports to develop many application layer protocols and standard routing protocols for connection-oriented and connectionless networks. Inbuilt it maintains all OSI and TCP/IP protocol stack, in NS-2 different functions are carried out at various layers of TCP/IP stack. The combination of C++ and TCL (Tool Command Language) makes NS-2 scripts. C++ is used as front end language and TCL as back end language. The beauty of NS-2 is anyone can add new feature or functions to it for their own purposes. Most of standard protocols are supports in this simulator, for example protocols like FTP,TELNET,DNS and HTTP etc.

3. ENCRYPTION AND DECRYPTION TECHNIQUES

1. DES (Data Encryption Standard)

Data encryption standard is works on 64 bits of block size and for the first time this algorithm is developed and proposed by IBM. The encryption procedure is separated into 16 stages and it includes eight S-Boxes.

DES has three steps –

- Shuffling of bits
- Moving with non linear substitutions
- XOR operation is carried out to get final output or a result.

The result XOR operation is combined with a particular round's sub key and the sub keys of reverse order for Decryption.

2. Triple DES

Triple DES is the enhanced form of DES algorithm. The overall length of key is 192 bits, and the each key is divided into 64-bits of three sub keys. Next technique is similar like DES algorithm but one major difference is that it repeats three times because of its 192 bits, working of keys as follows- first key encrypts the data, second key decrypts the encrypted data and finally third key again encrypts the decrypted data. It is also not so secure but it is good compared to DES.

3. RSA

One of the example for public key encryption is RSA algorithm. Triple DES is symmetric algorithm but, RSA is treated an asymmetric algorithm by the reason of its usage of two keys rather than single key, one key is used for encryption and other is for decryption. Usually Public key is used for encrypting the data and Private key for decryption. RSA is one of the complicated encryption technique that takes much more time to break.

4. Blowfish

Earlier in 1993, Bruce Schneier who has proposed this algorithm. amongst all available encryption algorithms it is one of the most efficient encryption technique. The length of the key begins from 32 bits to 448 bits, each block is size of 64 bits. This technique has two fundamental steps- first expansion of key, secondly each P-array consist of 18 sub keys of 32 bit. Totally it consists four 32 bit S-boxes where each S-box contains 256 entries, and lastly XOR function is used to encrypt the data. In this technique key is not frequently changed so it has more applications compared to others.

5. Two fish

Both Twofish and Blowfish is designed by same computer security expert, this twofish is successor of blowfish. Key

length in this technique is upto 256 bits and it is Symmetric key cryptography i.e single key is used for both encryption and decryption.

6. AES(Advanced Encryption Standard)

Several organizations are trusted this encryption technique, It is one the efficient encryption algorithm in 128-bit format. AES uses the two types of key lengths, one is 192 bits and other one is 256 bits for high level encryption purposes. AES is resistant to most of the attacks except brute force because brute force uses all possible combinations i.e 128, 192, 256 bit format.

7. RC4 Algorithm

The computer security expert Ronald Rivest who developed this algorithm. Here based on key sequence, the state entries will exchange. The length of key is ranges from 1 to 256 bytes. For encryption results into pseudo-random bytes to generate the stream, then the stream will be XORed to produce encrypted data. This RC4 encryption technique is 10 times quicker than the DES algorithm.

8. Diffie-Hellman Key Exchange

Diffie Hellman is an algorithm used to establish a shared secret communication between two parties. It is mainly used as a method of exchanging keys. If both the sender and receiver gets the same shared secret value then we can say that channel is secure for transmission.

Steps for Diffie- Helman key exchange-

Public Elements-

p -> Prime number

g -> g<p and g is primitive root of prime number

Alice's Key Generation-

Selection of Private key X_{Alice} $X_{Alice} < p$

Calculation of Public key Y_{Alice} $Y_{Alice} = g^{X_{Alice}} \bmod p$

Bob's Key generation-

Selection of Private key X_{Bob} $X_{Bob} < q$

Calculation of Public key Y_{Bob} $Y_{Bob} = g^{X_{Bob}} \bmod p$

Alice's Secret key

$K_{Alice} = (Y_{Bob})^{X_{Alice}} \bmod p$

Bob's Secret key

$K_{Bob} = (Y_{Alice})^{X_{Bob}} \bmod p$

If we get the same value for both KAlice and KBob then we can say channel is secure of transmission and the receiver is trustworthy to receive information or data

4. CONCLUSIONS

In the existing system, the security provided at the data link layer for large Ethernet networks using GKSP (Group based MAC key selection protocol). But this scheme has issues like security integration at network layer, efficient key sharing, node overhead. In this survey paper we concentrated on how data security will be carry out at Network layer by using the Security functions like Encryption, Decryption and Key exchanging algorithms in wireless network.

REFERENCES

[1] Prashant Kumar, Shivangi Maheshwari, Harsh Kumar Dubey, *"Development and Validation of a NS2 Protocol for Data Security at Network Layer*", International Conference on Computing, Communication and Automation (ICCCA2015), Pages: 529-534, Publication year-2015

[2] Sourabh Chandra, Siddhartha Bhattacharyya, Smita Paira, Sk Safikul Alam, "*A Study and Analysis on Symmetric Cryptography",* International Conference on Science, Engineering and Management Research(ICSEMR 2014), Publication year-2014.

[3]Shumin Xu; Yatao Yang, "*Protocols simulation and performance analysis in wireless network based on NS2*" Multimedia Technology (ICMT), 2011. Page(s):638 – 641,.Publication year-2011.

[4] Jiang Hong; Yu Qing-song; Lu Hui, "*Simulation and Analysis of MAC Security Based on NS2*" Multimedia Information Networking and Security, 2009.MINES _09. Volume: 2, Page(s): 502 - 505. Publication year-2009

[5] Vojislav B., Jun Fung, and Jelena *"MAC Layer Security of 802.15.4-Compliant Networks",* MASS 2005 Workshop – WSNS05, Publication year-2005