National Conference on New Frontiers of Engineering, Sciences, Management and Humanities
School of Electronics and Communication Engineering, REVA University, Bengaluru
REVA UNIVERSITY Bengaluru, India
12th-13th October 2018 www.conferenceworld.in ISBN: 978-93-87793-49-1

Security in MANET using SHA-512 and Blowfish Algorithm

[1]Prof. Prerna Rawat, [2]Prof. Pranali Deshmukh

[1]*Computer Engineering Department, G S Moze College of Engineering*

[2]*Information Technology, G S Moze College of Engineering*

ABSTRACT

MANET is self organizing, decentralized and dynamic network means node can move anywhere. Self organizing capability is advantage as well as disadvantage for MANET because host node can be router but if it is not in the network then it is difficult to transfer data by that node. The MANET is also used for big network and internet but now rapidly increase internet users worldwide to access global information and technology. I am using hybrid security algorithm in Blowfish with SHA algorithm in proposed system

Keywords: MANET, Global, Security.

I.INTRODUCTION

Now six billions people around the world access internet by any of field area network like 2G, 3G, 4G, LTE, wifi, Wimax, Mobile Broadband, wired, etc. They use the FAN for browsing the web, sending and receiving emails, accessing multimedia content, playing games, social networking and other tasks, so more peoples come to in connect to share global information and communication infrastructure. Passwords should **never**, ever, be stored encrypted. Encrypting something implies that it can be decrypted; if the key is discovered your stored password can be reverted back to plain text. The password should be salted and then hashed. Hashing is a one-way process, the only way to 'recover' your password is to guess the password and then, using the same salt, run it through the process used to generate the original hash. It may seem a subtle difference, but at the technical level, the challenges involved in brute-forcing a hash differ to that of decrypting cipher text.

Challenges

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.
- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.

Blowfish algorithm

Blowfish is a fast block cipher except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text.

Blowfish is a symmetric block cipher developed by Bruce Schneider. Blowfish makes use of a key that ranges from 32 bits to 448 bits. The key used to generate 18 32-bit sub keys and four 8×32 S-boxes containing a total of 1024 32-bit entries. The steps in generating the P-array and S-boxes are as follows:
Initialize first P-array and then the four S-boxes in order using
1. The bits of fractional part of the constant π.
Perform a bitwise XOR of the P-array and the K-array, reusing Words from the K-array as needed. Encrypt the 64-bit block of all zeros using the current P and S
3. Arrays; replace P1and P2with the output of the encryption. Encrypt the output of step3 using the current P and S arrays and replace P3and P4with the resulting cipher text. Continue this process to update all elements of P and then, in order, all elements of S, using at each step the output of the continuously changing Blowfish algorithm. In the encryption process [7] the plaintext is divided into two 32-bit halves LE0 and RE0.The variables LEi and REi to refer to the left and right half of the data after round i has completed. The encryption algorithm can be defined by the following
Pseudocode:

For i=1 to 16 do
REi=LEi-1 XOR Pi;
Lei = F [REi] XOR REi-1;
LE17=RE16 XOR P18
RE17=LE16 XOR P17;
In vice versa, we were performing Decryption process

SHA -512 Algorithm

The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993; the algorithm takes as input a message with a maximum length of less than 2128 bits and produces as output a 512-bit message digest [8]. The input is processed in 1024-bit blocks. The processing consists of the following steps.

Append padding bits

The message is padded so that its length is congruent to 896 modulo 1024 (length 896 mod `1024). Padding is always added, even if the message is already of the desired length. Thus the number of padding bits in the range of 1 to 1024. The padding consists of a single 1-bit followed by the necessary number of 0-bits

Initialize hash buffer.

A 512-bit buffer is used to hold

3. Intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialized to the following 64-bit integers (hexadecimal values)

Where IV= initial value of the adcdefgh buffer

Abcdefgh =the output of the last round of processing of the ith message block

N=the number of blocks in the message (including padding and length fields).

SUM64 = Addition modulo 264 performed separately on each word of the pair of inputs

MD=final message digest value

II.CONCLUSION

The MANET is already successfully run in our environment so with some minor changes and providing light weight cryptographic system, hybrid algorithm in proposed system achieve significant performance in all services like traffic management, smart cities, smart building, controlling, monitoring, logistics etc.

REFERENCES

1. Vikram M. Agrawal, Samip A. Patel, "A STUDY ON SECURITY LEVEL OF AD HOC ROUTING PROTOCOL TO FIND OTHER APPROACH WITH DSDV", in IJCET (IAEME) **4**(6), 240-246, (2013). ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online).
2. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," Security Protocols, 7th International Workshop, LNCS, Springer-Verlag, 2009
3. .Rhythm Dubey, Himanshu Gupta, "SQL filtering: An effective technique to prevent SQL injection attack", *Reliability Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) 2016 5th International Conference on*, pp. 312-317, 2016.
4. View Article Full Text: PDF
5. A technology roadmap of the Internet of Things, 4 April 2008, Appendix F of Disruptive Technologies Global Trends 2025 page 1 Figure 15 (Background: The Internet of Things), SRI Consulting Business Intelligence/National Intelligence Council
6. Zhang Hua,GaoFei,WenQiaoyan" A Password-Based Secure Communication Scheme in Battlefields for Internet of Things", *China Communications*, **8**(1),72-78,(2011).