Security of Wireless Mesh Network from Denial of Service Attack

Sunita Rani
Assistant Professor
BPSMV Khanpur Kalan (Sonipat)

Shweta Nijhawan
M.Tech Student
BPSMV Khanpur Kalan (Sonipat)

ABSTRACT
A wireless mesh network is correspondences arrange comprised of radio hubs sorted out in a mesh topology. It is additionally a type of wireless ad hoc network. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers & gateways. In this, discussed security issues related to Wireless Network. Then, study of Existing Security loop holes within wireless mesh based distributed network environment. Objective of research is to develop system to make Wireless mesh network secure form denial of service attack.

General Terms
Wireless Mesh Network, Denial of service attack, DES Algorithm, AES Algorithm, Security.

Keywords
Ad Hoc, Fiber optics, Co-axial cable, Wireless Cable.

1. INTRODUCTION
As different remote networks [1] advance into cutting edge to give better administrations, a key innovation, remote work organize, had developed as of late. Wi-Fi card in your portable PC may turn into a get to point to it perform part as system customer. Remote work organizes comprise of two hubs: mesh router & mesh client [2]. In mesh router, standing framework type of spine arranges and of work organizes inside couple of energy limitations. Mesh router could play out all extensions work as utilized as a part of regular remote switch. They bolster different remote interfaces and innovations.

2. DENIAL OF SERVICE ATTACK
Denial of service attack (DOS) is a consistent threat to sites. DOS had gotten expanded consideration as it could prompt an extreme lost of income if a site is taken disconnected for a significant measure of time. A dispersed refusal of-service [5] (DDoS) assault happens when various frameworks surge data transfer capacity or assets of a focused on framework, normally at least one web servers. Such an assault is frequently consequence of different traded off frameworks flooding focused on framework with movement. A java is a system of zombie PCs modified to get charges without proprietors' information [5]. At the point when a server is over-burden with associations, new associations could never again be acknowledged. Most imperative elements to an assailant of utilizing a spread dissent of-benefit assault are that numerous machines could produce more assault movement than one machine, many assault machines are harder to kill than one assault machine, and that conduct of each assault machine could be stealthier, making it harder to track and closed down. These aggressor favorable circumstances cause challenges for resistance systems

3. DES ALGORITHM
DES is a Private (symmetric) key cryptography calculation. In DES, General calculation plan 64 bit plaintext utilized as info and key is 56-bits in length [6]. Indistinguishable key is utilized for encryption and unscrambling. DES contains an assortment of operations: mixing of bits, substitution, exclusive OR, S- boxes, straight permutation and expansion permutation

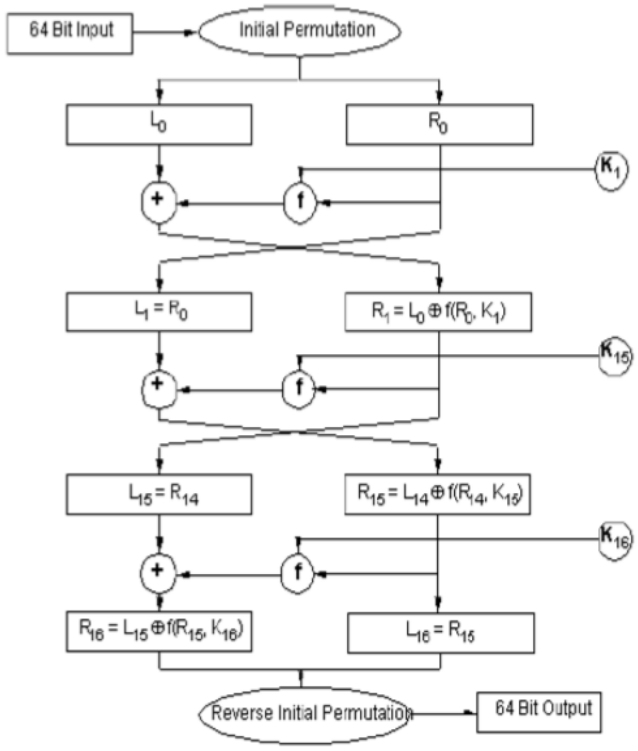

Fig.1 DES algorithm structure [6]

DES algorithm
Encryption (cont.)
Plaintext: X
Initial Permutation: IP( )
$Round_i$: $1 \leq i \leq 16$
32-bit switch: SW( )
Inverse IP: IP^{-1}( )
Ciphertext: Y
Encryption (Round) (cont.)

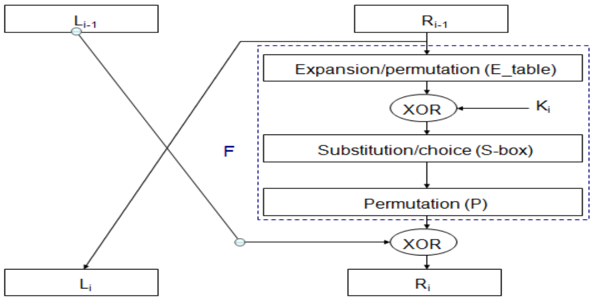

Fig.2 DES Algorithm

4. AES ALGORITHM

AES/Rijndael is an iterated square figure, implying that underlying information piece and figure key experiences different rounds of change before creating yield [7]. Each middle of the road figure result is known as a State. Encryption handle utilizes an arrangement of uniquely determined keys called round keys.

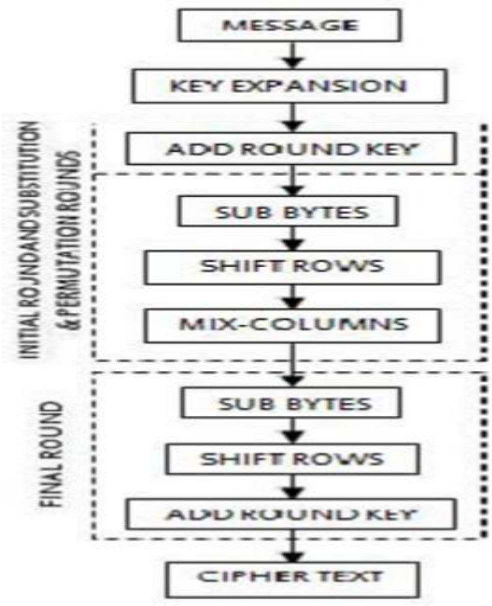

Fig.3 AES Algorithm [7]

Algorithm for Encoding to make Encryption in AES

1 Set array of tlb to 'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z','a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v', 'w','x','y','z','0','1','2','3','4','5','6','7','8','9','+','/'

2 take a string buffer

3 pad = 0;

4 i = 0

5 increase I by 3 until i is less than length of data and Repert step 6 to Step 15

6 perform And operation on data[i] with 0XFF store in k1

7 Perform Left Shift k1 with 16 and store in k2

8 Perform and operation on k2 and 0xFFFF and store in b;

9 if (i+1) is less than length of data than

i) Perform And Operation on data[i+1] with 0xFF and store in k3

ii) Perform Left Shift with 8 and store in k4.

iii) Perform Or operation with b and k4 and store in b

Otherwise increment in pad by 1.

10 if (i+2) is less than length of data than

i) Perform And Operation on data[i+2] with 0xFF and store in k5

ii) Perform Or operation with b and k5 and store in b

Otherwise increment in pad by 1.

11 set j to 0 and repeat until j is less than 4-pad, increment j by 1

12 perform And operation b and 0XFC0000 and store Result in k6

13 perform 18 bit shifting on k6 and store in c

14 Append buffer with tbl[c]

15 Perform 6 bit right shift on b.

16 set j to 0 and make increment in j by until j is less than pad variable, append "=" in buffer variable

17 Return the value of buffer variable

18 Algorithm of encode ends here

Algorithm for Decoding to make decryption in AES

1 Set matrix tbl = { -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, 62, -1, -1, -1, 63, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, -1, -1, -1, -1, -1, -1, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, -1, -1, -1, -1, -1, -1, 26, 27, 28, 29, 30,31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, -1 }

2 Get Bytes from data and set bytes in bytes array.

3 Set i=0 and repeat following until i is less than length of bytes

Set b = 0

4 if tbl[bytes[i]] is not equal to -1

5 Perform And operation with tbl[bytes[i]] and 0Xff and Set in k1 and shift 18 bit and store in b

Other wise

Increment i by 1 and continue

6 Set num = 0;

7 if (i + 1 < bytes.length && tbl[bytes[i+1]] != -1)

Perform b= b | ((tbl[bytes[i+1]] & 0xFF) << 12)

Increment num by 1

8 if (i + 2 < bytes.length && tbl[bytes[i+2]] != -1)

An uncommon capacity issued by having bending and picture subroutines utilized as secret word keeping in mind the end goal to spare watchword from disconnected lexicon assault. Work is executed in one of major utilized dialect named java. form calculation b = b | ((tbl[bytes[i+2]] & 0xFF) << 6);

Increment num by 1

9 if (i + 3 < bytes.length && tbl[bytes[i+3]] != -1)

Set b = b | (tbl[bytes[i+3]] & 0xFF)

Increment num by 1

10 Repeat step 11,12,13 until num > 0

11 Set c = (b & 0xFF0000) >> 16;

12 Write c in buffer

13 shift 8 bit in b

14 Decrement num by 1

15 Increment 4 by i and store in i

16 Return value of buffer

5. SECURITY OF WIRELESS MESH NETWORK FROM DOS ATTACK

Symmetric Key Cryptography

Utilization of Internet is developing rapidly [11]. Along these lines, giving security to information over systems had turned into a basic issue these days. Information over systems is shaky; it ought to be unveiled just too proposed beneficiaries not to everybody. Information is more inclined to assaults while transmitting in organize. Cryptography [11] appeared to give answers for all issues of system security. Server verify client and client confirm server creating an extremely solid session key utilizing their mutual secret word over an uncertain channel by utilizing symmetric figure.

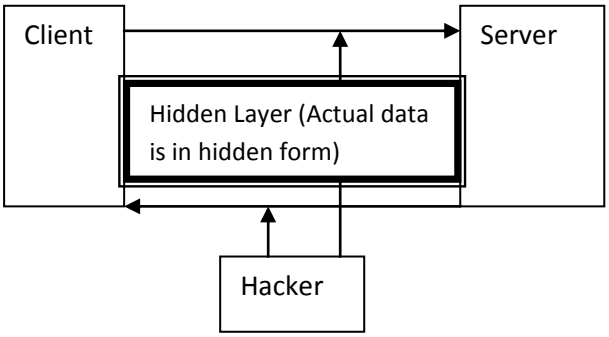

Fig.4 Proposed Model

An uncommon capacity issued by having bending and picture subroutines utilized as secret word keeping in mind the end goal to spare watchword from disconnected lexicon assault.

Work is executed in one of major utilized dialect named java.

Encryption Steps

Step 1 Encryption of plaintext that is to be send by sender using encryption from secret Key which is actually sender's private key & thus generating cipher text using DES.

Step 2 Further, it would carry out procession secret Key which is receiver's public key & thus encrypting algorithm.

Step 3 A digital envelop is sent to receiver having cipher text & Key so encrypted.

6. PROPOSED SECURITY OF WIRELESS MESH NETWORK FROM DOS ATTACK

1. Here IP filter to reject unauthenticated transmission of packets from server to client.
2. Here enhance network security by customizing existing encryption techniques.
3. To enhance loopholes of open security mechanisms & enhance security of network.
4. To program of corresponding & socket server client to prevent unauthentic access during data transmission.
5. To make use of more complex key during encryption & decryption.
6. To develop user interface to make client server communication.

OTP GENERATION

One time password would be generated randomly by Math random() function in java. Each & every time complex OTP number could be generated to be used during decryption.

IP Filter

Centralized database of IP address would be created on centralized server & decryption request from authentic IP would be accepted. If IP had been not found in database or its status had been 0 then Decryption would not be allowed.

In proposed model there would be triple layered security

1. Security layer 1 would be customized cryptography algorithm of AES to enhance security by integrating XOR operation in it.
2. Security layer 2 would drop packets from unauthentic IP addresses.
3. Security layer 3 would authenticate user by providing login password security at application layer.
4. Security would be enhanced using one time password also that becomes useless after using one time.
5. In this way we would secure wireless network from external attacks & authentic access.

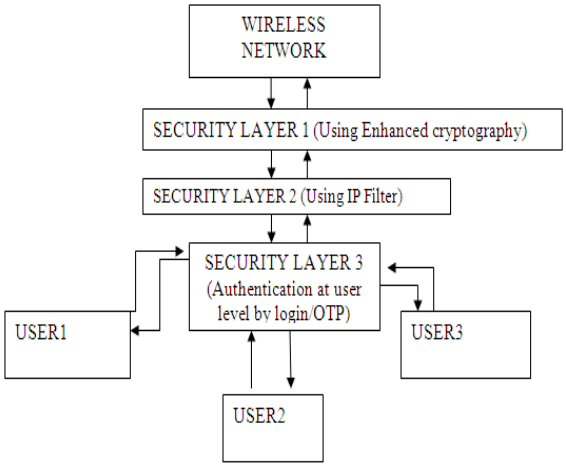

Fig.5 Triple Layer Security

7. IMPLEMENTATION

Create a new application project by selecting File New Project in java le window or via a command prompt. You could do this using user interface building blocks to piece together a user interface. Create a new project of type Forms Application

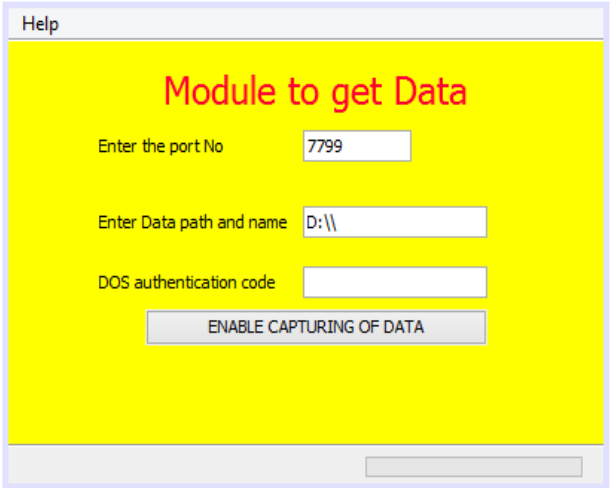

Fig.6 Module to get Data using particular port & DOS Authentication code

This module is designed to provide security against DOS attacks for this different techniques are used. It uses a simple model to send data in encrypted form which is decrypt at receiver. Firstly it read data from file and encrypted with different techniques. Here a simple encryption technique is

used like XOR ing. Firstly data bits read from file is XOR with Triple Layer Security the given authentication code and send data to receiver. Receiver who only knows the encryption technique and authentication code will retrieve the original data otherwise the data gets corrupted.

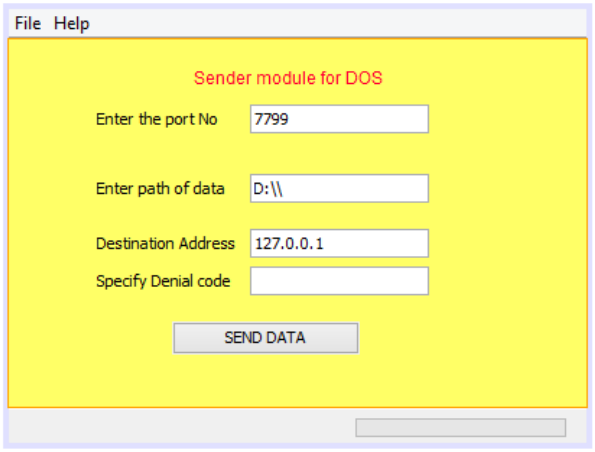

Fig.7 Module to send data using particular port & at particular Location using Specific DOS authentication code.

7.1 Comparative analysis of traditional & proposed dos prevention system

The proposed work done is far better as compared to traditional as packet transmission is fast & probability of dropping packet is less as we have used customized port & data is kept secure using DOSDECODER logic. Packet becomes difficult to trace by hacker. So probability of denial of services gets reduced in case of proposed work. Proposed model is easy to operate as it is in form of Graphical user interface that is user friendly.

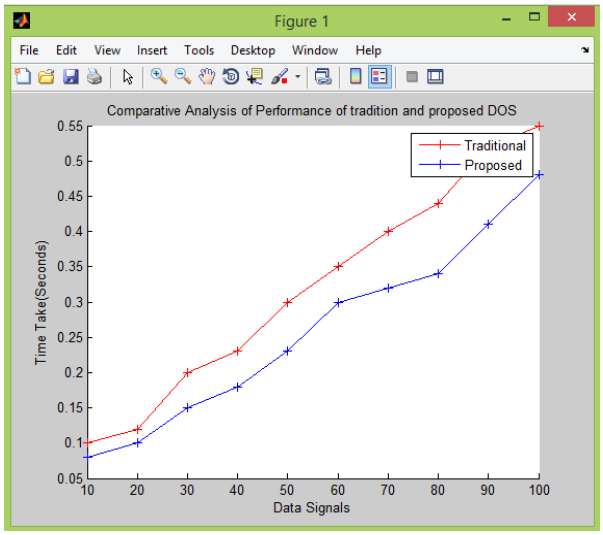

Fig.8 Comparative analysis of traditional & proposed dos prevention system

7.2 Comparative analysis of packet droping during traditional & proposed work

Proposed work done is much better than the traditional approach in terms of loosing data packet, transmission speed. In this custom ports are used instead of specific ports to prevent it from intruders attack. As the common ports are easily hacked by intruders and also the data is secured using DOSDECODER logic. To show its performance, draw a graph between data signal and time taken to transfer data.

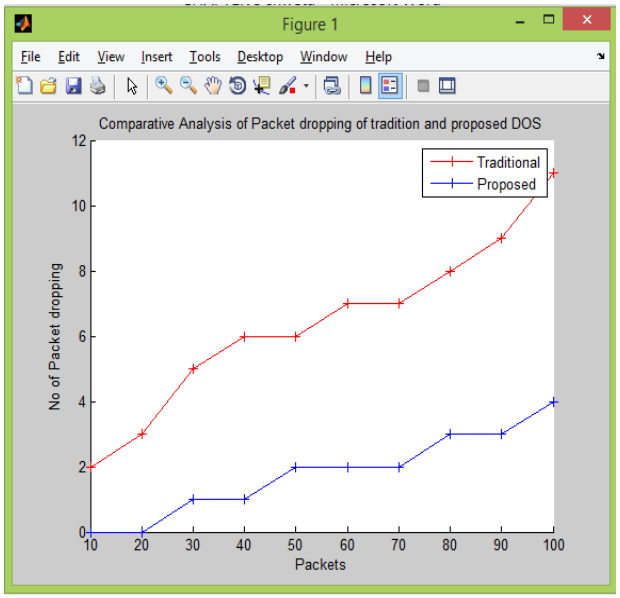

Fig.9 Comparative analysis of packet droping during traditional & proposed work

8. CONCLUSION

The wireless sensor systems proceed to develop and turn out to be broadly utilized as a part of numerous applications. Along these lines, the requirement for security ends up plainly imperative. In this paper, focus on Symmetric Cryptography because of the suspicion that symmetric cryptography has a higher adequacy and require less vitality utilization, as opposed to open key cryptography. In this broke down the Advanced Encryption Standard (AES) which applies numerous complex numerical counts on plain content utilizing 10 rounds to give the subsequent figure content. Additionally the time required for encryption is less. Issue of ad hoc system security is request of day. Proposed execution had upgraded security of specially appointed system. Port is server started that is not unmistakable to programmer and he would Data transmission could be made more secure from programmer to by scrambling information on sender side and decode it on customer side. To play out this we have to consolidate two advancements.

What's more, on part of java assume its best part to create GUI interface to make framework simple to work by client Socket Programming and Data Encryption.

9. REFERENCES

[1] Anil Kumar Gankotiya , Sahil Seth , Gurdit Singh , "Performance Analysis of Secure Wireless Mesh Networks" , Research Journal of Recent Sciences Vol. 1(3), 80-85, March 2012 .

[2] Monika, "Denial of Service Attacks in Wireless Mesh Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (3), 4516-4522, 2012.

[3] Priya Maidamwar & Nekita Chavhan, "security issues to detect wormhole attack in wireless sensor network", International Journal on AdHoc Networking Systems (IJANS) Vol. 29(4), 37-50, October 2012.

[4] Pooja Sharma, "performance analysis of secure wireless mesh networks" International Journal of Research in Science & Technology (IJRST) 2013, Vol. 3(4), 65-75, 2013.

[5] Khaled M.Elleithy, Drazen Blagovic, Wang K. Cheng, Paul Sideleau, "Denial of Service Attack Techniques: Analysis, Implementation & Comparison", Journal of Systemics, Cybernetics, & Informatics 3.1, 66-71, 2005.

[6] Manjula K G, M N Ravikumar, "Color Image Encryption & Decryption Using DES Algorithm", International Research Journal of Engineering & Technology, Vol. 03(07), 1715-1718, 2016.

[7] Madhumita Panda, "Data Security in Wireless Sensor Networks via AES Algorithm" IEEE Sponsored 9th International Conference on Intelligent Systems & Control, 2015.

[8] Yanchao Zhang & Yuguang Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks",IEEE journal on selected areas in communications, vol. 24(10), 1916-1928, 2006.

[9] Ian F. Akyildiz, Xudong Wang, Weilin Wang "Wireless mesh networks: a survey", Computer Networks, Vol. 47, 445–487, 2005.

[10] Li, S., Zheng, X., Mou, X., Cai, Y, "Chaotic encryption scheme for real-time digital video", In: Real-Time Imaging VI. Proceedings of SPIE, vol. 4666, 149–160, 2002.

[11] Priti Bali1, "comparative study of private & public key cryptography algorithms: a survey", IJRET: International Journal of Research in Engineering & Technology , Vol. 03(09) ,191-195, 2014,

[12] Haroon Shakirat Oluwatosin, "Client-Server Model", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16(1), 67-71, 2014.