IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Reconnaissance For Packet Rerouting In Wsn

[1]G M Lakshmi Prasanna,[2]B P Sowmya

[1]Research Scholar, Dept. of MCA, PES College of Engineering, Mandya, Karnataka.
[2]Assistant Professor, Dept. of MCA, PES College of Engineering, Mandya, Karnataka.

Abstract: **In Wireless Sensor Networks, data collecting is one of the most important features (WSNs). Despite the fact that various novel ways to data gathering have been proposed over the last decade, it remains a hot research topic with a number of significant hurdles. One of the shortest path techniques in wireless sensor networks is Dijkstra's method.The virtual proxy network delivers data within the server. When you connect to a VPN, you're essentially establishing a tunnel between your device and the VPN server of your choice, encrypting all data sent and received. Virtual private networks (VPNs) let organisations to construct secure, end-to-end private network connections over third-party networks like the Internet rather than having separate Leased lines by utilising contemporary encryption techniques such as 3DES and tunnelling. We employ techniques to determine the shortest path and encrypt data shared on the server in this work.**

Index Terms **- Wireless Sensors Network, Data routing, Proxy network, Triple DES, MD5**

I. INTRODUCTION

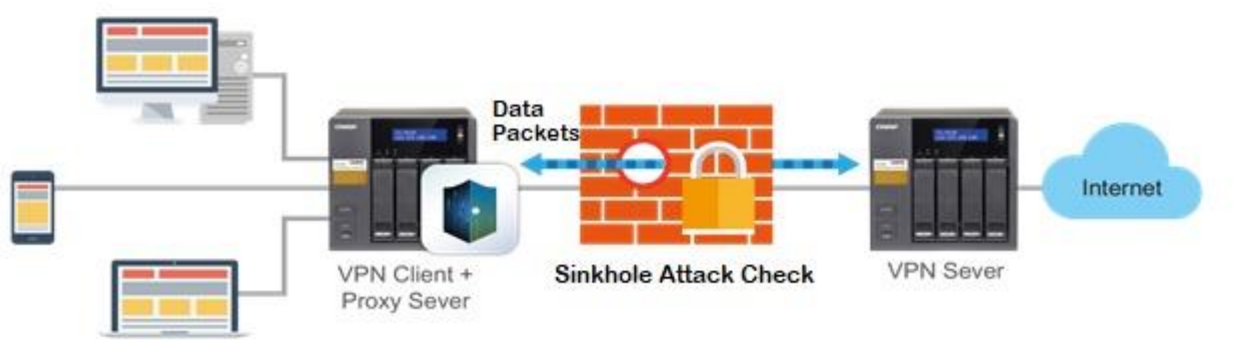
In terms of integration and development, wireless sensor networks are a new development direction in the field of communication that brings together traditional and emerging fields. Wireless sensor networks are used in a variety of industries, including medical and health care, military surveillance, target tracking, and people's lives, because of their advantages of ease of deployment, low cost, and effective camouflage. The data is exchanged in the server with the help of a proxy server, where it is completely safe and delivered from one node to another in less time. The information that needs to be communicated is divided into packets and transmitted to the server. Unauthorized individuals will be unable to track down the data because the user will connect to the server over a proxy network. The information is divided into packets, which are then encrypted and sent to the destination node through algorithms. An algorithm is used to find the shortest path from the originating node to the destination node, allowing data to be transmitted in less time and with more security. The packets are encrypted and subsequently decoded, making the data untraceable. When a user shares files on a server or network, the proxy network generates a key that the user can use to access the server and do operations. As a result, the server user is protected by the proxy network.

II. LITERATURE SURVEY

Karthik .S, Muruganandam .A[1] et al presented a paper that shows how the triple des work. This paper describes a cryptographic approach for private communication. It is a method for safeguarding sensitive information. A block cypher based on two cryptographic methods, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA), is used to encode the secret message. With a block length of 128 bits and a key length of 256 bits, this algorithm outlines the mathematical steps required to change data into a cryptographic cypher and then back to the original form.D. Coppersmith[2] propose a new mode of multiple encryption—triple-DES external feedback cipher block chaining with output feedback masking. The aim is to provide increased protection against certain attacks (dictionary attacks and matching ciphertext attacks) which exploit the short message-block size of DES. The new mode obtains this protection through the introduction of secret masking values that are exclusive-ORed with the intermediate outputs of each triple-DES encryption operation.Alok Kumar Kasgar, Mukesh Kumar Dhariwal[3], presented an paper on MD5 algorithm and how it works and what are the uses of this algorithm. The paper has full information about the MD5 algorothim. They also concentrated the new way to use this algorithm.This paper solves the security problems in Wireless Sensor Networks by introducing energy via external batteries, which extends the sensor network's lifetime. It also detects the black hole attack in routing from source to destination and proposes a solution based on public key encryption via the message digest algorithm. It increases network black hole detection and packet transfer. The simulation findings suggest that qos parameters such as packet delivery ratio and end-to-end delay throughput can be used to detect a black hole assault[4]We focus on data security in cloud computing in this work, and we provide an attribute-based proxy re-encryption system with keyword search (ABPRE-KS) to allow for flexible and secure data sharing among cloud users. An access structure consisting of numerous attributes describes a user's access privileges in our scheme, whereas cypher texts are tagged by several target attributes. Without disclosing any critical information to the cloud server, a delegator can convert the original cypher texts into proxy cypher texts encrypted by the delegate's attributes. A delegate may also make a search request on the cypher texts if his credentials meet the delegate's access policy.[5]

III. PROPOSED SYSTEM

The suggested solution explains how to share files across a VPN. The decryption key is more powerful since it can decipher several cypher messages without growing in size. According to the problem statement, “to design an efficient public-key encryption scheme that supports flexible delegation in the sense that any subset of the cypher texts (produced by the encryption scheme) can be decrypted by a constant-size decryption key (generated by the owner of the master-secret key”). A new sort of public-key encryption known as key-aggregate cryptosystem was created to overcome this problem.



IV. METHODOLOGY

Working Of Triple Des Algorithm

The realistic approach was to alter the way DES is used rather than altogether abandoning it. As a result, Triple DES schemes were adjusted (sometimes known as 3DES). In addition, there are two types of Triple DES: 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES) (2TDES).

The following is the encryption-decryption procedure:

- Using single DES with key K1, encrypt the plaintext chunks.
- Using single DES and key K2, decrypt the result of step 1 now.
- Finally, encrypt the result of step 2 with key K3 using single DES.
- The ciphertext is the result of step 3.
- A ciphertext's decryption is a backwards operation. K3 is used to decrypt, then K2 is used to encrypt, and finally K1 is used to decrypt.

Working of MD5 Algorithm

The MD5 message-digest algorithm is the fifth version of Ron Rivest's Message-Digest Algorithm, which generates a 128-bit message digest. MD5 is much faster than other message digests, as it takes plain text of 512-bit blocks, divides it into 16 blocks of 32 bits each, and produces a 128-bit message digest, which is a set of four blocks of 32 bits each. MD5 generates the message digest in five steps: padding, append length, dividing the input into 512-bit blocks, initialising chaining variables, process blocks, and four rounds, and utilising a new constant in each iteration.

```
Input:C1,C2..Cn
for(i=1;i<(n+1);i++){
    if(Ci!=null) {
        if(Prefix mutual relations){
            ascending order;
        }
        Insert Pmin into root node;
        Follow the ascending order insert the rules;
        Insert others into the right subtree;
        Construct the second Layer;
    }
    Return trie structure;
}
if (Dmin-dist(Mp.Mm))
    {(Return Cm;)}
if (Prefix mutual relations)
    {Search the left subtree;}
Else
```

19: {Search the right subtree:)
20: Return Rm;

V. CONCLUSION

Our major goal is to set up a VPN network without spending a lot of money or time. This is useful for two or more people who want a private network to safeguard their data and the network from prying eyes. While firewalls help to prevent unauthorised individuals from leaving and entering an organisation, they do little to protect against threats on the Internet. Hackers and potential e-criminals can see sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, and so on. This is when the VPN's advantages can be seen. At its most basic level, a VPN is the ability to utilise the public Internet in a safe manner as if it were a private network. Users encrypt their data and identities with a VPN to prevent unauthorized persons or computers from viewing or tampering with the data.

REFERENCES

[1] Karthik.S,Muruganandam.“A Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System”

[2] D. Coppersmith, D. B. Johnson, S. M. Matyas “A proposed mode for triple-DES encryption”. IBM Journal of Research and Development

[3]Alok Kumar Kasgar, Mukesh Kumar Dhariwal “A Review Paper of Message Digest 5 (MD5)” International Journal of Modern Engineering & Management Research.

[4]Hanshu hong, zhixin sun “towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search”

[5] K.Marimuthu,D.Ganesh Gopal, K. SashiKanth “Scalable and secure data sharing for dynamic groups in cloud”

[6] Jiang Zhang, Zhenfeng Zhang “Secure and Efficient Data-Sharing in Clouds”

[7]. Xinmiao Zhang and Keshab K. Parhi,”Implementation approaches for the advanced encryption standard algorithm”, IEEE transactions.

[8] “Advanced encryption standard (aes)”, federal information processing standards publication 197.
huang and fanzheng kong.the research of vpn over wlan

[9] Huang and fanzheng kong.the research of VPN over WLAN

[**10]**Sanchez-garcía, j.García-campos, j.Arzamendia, m,Reina, d.Gregor, D. A Survey On Unmanned Aerial And Aquatic Vehicle Multi-Hop Networks: Wireless Communications, Evaluation Tools And Applications. Comput. Commun. 2018, 119, 43–65.