International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Network and Data Security using Onion Routing Protocol with Salt Method & Used Wireless Mesh Network

Er. Ritu Aggarwal
HOD, MTech. (CSE), Himalayan Group of Professional Institutions , Kala Amb, Himachal Pradesh, India

ABSTRACT

Electronic communication is becoming an important issue now's day. Hiding the details of communication, content, nodes from the adversaries like an eavesdropper, hacker etc is usually not considering before. Encryption is becoming the most important part of all the communication channels. Onion routing is an anonymous connection that can provide support anonymous mail as well as other applications. The nodes include in the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. Onion routing with salt is the secure network topology that help to protect the data and the network after the enemy captures the node path. Onion routing with salt make the network more secure and data more protected. To create this and provide main aim of onion routing its uses public key encryption with salting method to put multiple layer of encryption around the original data thus making an onion like structure and each layer between source to destination peel off each layer of encryption. The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment. Registered users can connect to the network from anywhere a router or another connected user is available without being identified or tracked. The onion routing network Tor is undoubtedly the most widely employed technology for anonymous web access which also gives good security for anonymous transmission of data

Keywords : Onion, Salt, Encryption, Security TOR

I. INTRODUCTION

Onion Routing : Onion routing was first proposed by Reed, Syverson and Goldschlag . In onion routing, for a given connection, the sender selects a sequence of routers, known as a circuit, that will be used to forward the sender's traffic. The sender establishes a circuit by first directly opening a circuit with the first router, and then iteratively extending the circuit by sending message over the existing circuit. Messages are encrypted with the key of each router in the circuit in the reverse order that the routers appear. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message. In the original onion routing protocol [12], each onion router is equipped with a pair of public and private key. The source uses the public keys of the intermediate routers with the top layer encrypted with the public key of the router immediately next to the source. The intermediate routers then use their own corresponding private keys to decrypt the packet and obtain the information about the next hop in the network. The packets thus routed and forwarded by each intermediate genuine node, eventually reach the destination. The advantage here is that if any one of the routers is compromised by an adversary, even then, the other components remain beyond the reach, because of being encrypted using a different public key.

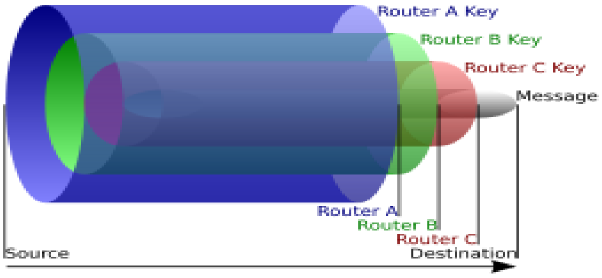

Fig 1.1 Onion Routing Protocol

Onion routing was initiated by Sun Solaris with implementation for web browsing, remote login process and sanitizing the user information from the browser while transmitting information through data packets. Onion routing promises to protect the integrity and confidentiality of data from the theft, eve dropping over the network and internet, onion routing proceed a devised a technique to limit the knowledge of information as possible while high level of anonymity is achievable. Onion routing have ability to work against the traffic analysis attack mainly because of there is no direct communication between sender and receiver. As it initiates a communication with an application specific router called onion routing proxy that was enough to manage TCP and Sock request of the client. Routing onion is a data structure designed by wrapping a plain text message with the successive layer of encryption such that each layer can be unwrapped by an one intermediary and no other can decrypt it. Onion routing is implemented with the help of encryption in the application layer of network in the communication stack like the layer of an onion. Tor help in encryption of original data including the IP address and send to the destination through a virtual circuit comprising successive, randomly selected. Each relay decrypts the layer of encryption to obtain only the successive relay in order to transmit the data. The final relay decrypts the innermost layer of encryption and sends the original data to its final destination without revealing and hiding the information of sender.

Result in many destruction of messages one for each anonymous connection that was suppose thorough that longstanding connection . Second problem is Expensive i.e. Onion message packets are in the sequences of cells that must be processed together. This onion processing involves a public key operation which is relatively very expensive in all other cryptographic. The third problem is Data Latency its means that delay in data. Data latency is also the main problem in the onion routing protocol. Message has been transmitted to may circuit and latency may be happen sometimes. Eve dropping is the forth problem that means an attacker can start monitoring the system when an onion router incoming queues and outgoing queues are empty so that attacker can determine the order in which marker arrives at a onion router Traffic Cost is also include in the problem. Traffic analysis to be cost of brute force attack on the cryptographic algorithms un reasonable [4]. Compromised nodes can cooperate to uncover the rout information to the outsider that was the main problem .Accessing a remote onion router does not really provide a protected anonymous environment because connection between the machine and onion router is not protected.

1.1 **Security architecture** : Security Architecture is aimed at providing complete anonymity to honest users. It will provide complete transmission of data from source to destination. Our system will aim at providing pseudonym approach to ensure network access anonymity and location privacy. In addition to the anonymity scheme, other security issues such as authentication, key establishment, and revocation are critical in WMNs to ensure the correct application of the anonymity scheme system it consists of Unconditional Anonymity and traceability done by Ticket based model provides the user privacy in the strongest sense and the user accountability. A WMN, consists of mesh clients and mesh routers. Mesh routers have minimal mobility and form the mesh backbone for mesh clients. Furthermore, in order to further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In addition, the bridge/gateway functionalities that exist in mesh routers enable the integration with other networks.

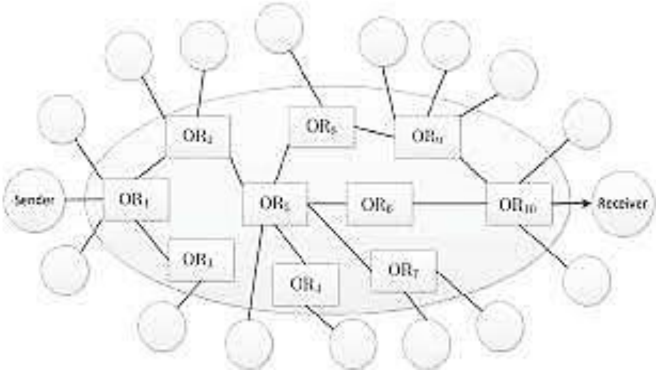

Fig1.2 TOR Routing by Onion Salt Method

TOR is the descendant of the onion routing project work by the project had many concept in it. TOR is a collection of onion routers which may have different functionality and roles in the network and during the network communication they perform their roles. Each router send an information in a secure way to next hop in the TOR network connection whereby if any single nodes is compromised then this been will be not affected anonymity as well as data communication send to and from the sender and receiver is work properly. TOR main aim is to hide the communication between the initiator and the target host fir which the initiator needs to communicate with the nodes [3]. The Tor network is an network in which each onion router runs as a normal and perform their usual duties without having any special type of privileges. A TLS connection is maintain for every other onion router. Each user can fetch their directories and establish circuit across the network and handle difficulties in handling connection from user application. Each router in the Tor maintain a long term identity key and short term identity key that is use to sign as TLS certification Salt is not only a single hash function, it is all about using more than one hash function among more the one hash function. Salt is the process of selecting a unique hash function from many hash function that are also known to server. Salt is also be added to make it more difficult from an attacker to break in a system by using password hash matching strategies because adding salt to a password hash prevent an attacker from testing known dictionary words across the entire system. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system. Hash = (salt + password) Verifier = salt + hash (salt + password) Diffie Hellman Exchange - It is protocol that help to maintain data integrity by exchanging a secret key between two users. Two users may be one is server and one client.

Basically MANET is mobile nodes collection, which communicates with other nodes by broadcasting. In Mobile adhoc networks, they do not have any central administration and existing infrastructure [1]. Therefore, the Mobile Adhoc Network (MANET) is using a temporary network communication. Mobile Adhoc Network (MANET) is working without infrastructure, so nodes in wireless network dynamically form their own network and connection on the flying movement. In wireless communication all nodes can listen to the communication if it is in sending range [2]. These wireless network nodes use some default routing protocols to identify the sender and receiver for every message. In wireless mobile adhoc network security is a major issue, particularly in military application. Now days this problem is going serious over the node mobility. Already various approaches have proposed to handle this security problem [3]. But now there is no routing algorithm is suitable for the environments. Over some years, more number of networks has been proposed with onion routing technique and some networks have been implemented. Onion routing [4], is a technique where message are covered in multiple encryption layers, forming an encryption like onion. In this scheme delivering message to destination by a no of intermediate onion nodes or routers, each intermediate router and node is responsible to decrypt one layer, and forward the packet or message to next router or node. A common process of an onion routing scheme is classify a collection of nodes that relay users of the system traffic. Users of this scheme then randomly select a path over the onion routers network and form a circuit, a sequence of nodes which will route traffic. After formed the circuit, each nodes in the circuit shares symmetric to user, that key will be used to encrypt future onion layers. In this proposed system we present onion routing protocol and Advanced Encryption technique. In that First network is constructed with n no of nodes [6]. After that nodes in the network can request data packet to other nodes. We can simulate nodes in the networks are moving because of the nodes mobility property. All nodes are maintained to forward data packet to other nodes. In this proposed scheme, discovering the shortest path is first process, and sends the packets to other node. When nodes come for registering into to the network, they get id and other information [7]. In this multi hop route forwarding is used to identify shortest path detection and Advanced Encryption Standard algorithm is used to achieve encryption process. Data is encrypted using Advanced Encryption Standard (AES) technique with primary key of all intermediate nodes. The wholesome is forwarded to first node, where the first decryption will be done by that node decryption key. In this proposed system, source node transmits the encrypted data packet to intermediate.

II. RELATED WORK

A paper is published by Uma Somani, Kanika Lakhani and Manish Mundra in Cloud discussion of that we have problem like security of data, files system, host security etc[1].They have proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue. Anonymous Connection and onion routing by paul and david specify of onion routing system, vulnerability analysis based on specific and performance result.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom proposed to generate RSA Public keys and Private Keys for public and private access to overcome the problem of data security. Certificate Binary file is used inside control node configuration file to make sure cloud data flow securely. The control node sends data through Secure Socket Layer after certificate activation. Finally AES algorithm is used for encryption .This unique combination makes this solution best to prevent different types of attacks. Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments.

Wei Liu, Member proposed that the route request packets are authenticated by a group signature, to defend against potential active attacks without unveiling the node identities. The key encrypted onion routing with a route secret verification message is designed to prevent intermediate nodes from inferring a real destination.

Later, Fan et al. [7] introduced the concept of anonymous multi-receiver IBE (AMRIBE) scheme and proposed an efficient AMRIBE scheme from bilinear parings. In an AMRIBE scheme, one can examine whether himself is a selected receiver or not. Nobody, except the sender, knows who the other selected receivers are. Subsequently,

Chien [8] pointed out that Fan et al.'s AMRIBE scheme only provides receiver anonymity for outsider attackers or non-selected receivers, and presented an improved AMRIBE scheme. However, only heuristic arguments for security proofs are presented. Tseng et al. [9] proposed a new AMRIBE scheme that was proved to be semantically secure against adaptive chosen ciphertext attacks in the random oracle model under the Gap-BDH assumption.

Wu and Li [1] propose a private routing algorithm, the called Onion Ring that is based on the Onion routing algorithm [2] that is designed to achieve privacy in wired networks. In the Onion Ring approach whenever a mesh node wants to be connected to the Internet it has to send a request to the Mesh Gateway. Then, the Mesh Gateway selects a route, and uses shared keys between itself and Mesh nodes (symmetric keys) nodes in the route to construct an "Onion", and delivers the "Onion" toward the initiator. Security analysis shows that the "Onion" structure protects the routing information from inside attackers. Due to open medium, the routing protocols are constantly victims of attacks trying to compromise their capabilities. Therefore the routing protocol used inside a mesh should be secured against attacks. To obtain these goal researchers proposed either mechanism to enhance existing routing protocols used for ad-hoc networks or new security protocols that are suitable for WMNs. Ben-Othman and Benitez [3], [4] propose an Identity Based Cryptography (IBC) mechanism to increase the security level of the HWMP. The authors propose two modifications trust management for internal nodes and digital signature of routing messages with IBC for external nodes. The use of the IBC eliminates the need to verify the authenticity of public keys and ensures the integrity of the control message in HWMP. Simulation results show that the IBCHWMP does not induce a long overhead compared to the original HWMP protocol. Based on the previous related studies, Anonymity, traceability along with Blind Signature is a suitable solution for providing security in wireless mesh networks. Previous work focused on Jin yuan [5]

Chi-Yin Chow [6] Monitoring personal locations with a potentially untrusted server poses privacy threats tothe monitored individuals design in network location anonymization algorithms, namely, resource and quality-aware algorithms that aim to enable the system to provide high quality location monitoring services for system users, while preserving personal location privacy.

Taojun Wu [8] Preserving Traffic Privacy in Wireless Mesh Networks mesh network privacy preserving architecture targets two privacy issues: Data confidentiality aims to protect the data content from eavesdropping by the intermediate mesh routers using cryptography-based approach traffic confidentiality prevents the traffic analysis attack from the mesh routers, which aims at deducing the traffic information.

David chaum [7] In general, a blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer.

III. PROPOSED WORK

This project aims at providing a basic approach for implementing data security for wireless mesh network. Network with a target of providing security to the data by using onion routing algorithm for wrapping, unwrapping the data and RSA cryptography for encryption and decryption. It strives to provide data security from client to server.

Methodology Method 1: Creation of Network Topology

- In this module we create two forms.
- First form is created where users can enter the source and destination for the transmission of data in the network.
- The second form will display the number of nodes, routers and gateway in the network. Method . Transmission of data from source to destination
- We have considered static architecture where there are 6 nodes in the network and 2 routers, 1 gateway formation in the network. Limited to static structure because of using onion routing algorithm for transmission of data.
- Static structure is predefined.
- User can send the data from source to destination and the data will be encrypted while sending and data will be decrypted after receiving by using RSA algorithm.
- Here wrapping and unwrapping of the data take place while transmitting the data from source to destination by using onion routing algorithm.
- The source and destination will change for each time.
- When there is loss of data from source to destination file will not reach the destination , Method 3: Algorithms used for data security
- RSA algorithm for encryption and decryption of the data.
- Onion routing algorithm for wrapping and unwrapping of the data before sending and receiving [4]

Secure Onion Routing Algorithms

Onion Routing Algorithm Steps:

Step 1: Network Setup: starts the Onion Router servers and establishes the longstanding connections between Onion Routers .

Step 2: Routes data randomly.

Step 3: Starting Services 1: Convert the file into ASCII and swap the characters.

Step 4: Starting Services 2: Wrap the data at each node it passes and unwrap before receiving the data.

Step 5: Connection Setup: Client establishes anonymous connection with host server.

Step 6: A router knows only its predecessor and successor.

Step 7: Data transfer: Transfer of data from client to server

All this process is implemented to provide security in avoiding data modification at the end of server side. For the same purpose two different servers are made and maintained one for storage server for storing user data file and second is for rehashing user password. When a user want to transmit a file to the server of the onion networks firstly key are exchange using our first process diffie Hellman key exchange process at the time of login [2]. Finally user's data file is encrypted using cryptographic algorithm with salt and only then it is going to be transmitted on network. Steps 1: Picks nodes from a list of nodes-the chosen nodes are ordered to provide a path that forming a circuit through which the message may be transmitted.

Step 2 :Using asymmetries key cryptography with salt, entry node uses public key to sends the encrypted message creating a cell calls create cell. 1-An create cell have2-The originator's half a diffie Hellman handshake 3-A circuit id Diffie Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This shared could be a password or a big number or an array of randomly chosen bits.

Step 3: 1-The entry node which just received the handshake, replies to the originators with:

2-The entry nodes' half of the handshake 3-A hash of the shared secret

Step 4: The originator and the entry node use their shared secret for encrypting everything.

Step 5: 1-The originator send s the entry node relay-extend cell for the next nodes using public key .

2-The originator's half of the differ Hellman handshake, a circuit id, a request.

Step 6: -The relay nodes then replies to the handshake.

Step 7: -Similarly the chain is extended further.

IV. Implementation

All this process is implemented to provide security in avoiding data modification at the end of server side. For the same purpose two different servers are made and maintained one for storage server for storing user data file and second is for rehashing user password.

I: Implementing the encryption algorithms with salt.

II: Connection Establishment.

III: Data transfer The first step starts with implementation onion routing encryption algorithms adding salt in it. There are many different algorithms are used for connection establishment and data transferring. RSA algorithm is used for establishing connection. It is the standard public key cryptography algorithm and cipher text are not easily decrypted, because the process of decryption is not an inverse process of encryption.. Random prime numbers are generated for encryption and decryption. Using system time onion key is generated. While sending the onion keys are generated that made difficult to predict the keys. TCP socket connection is used for connection. For anonymous communication and private is to be performing first. So the path that is to be followed by the sender and receiver and the address of the proxies through they pass during connection. The first layer of onion decrypted at its intermediated proxy and appropriate details such keys, IP address and the function for decrypting the data that will be build into routing table. As connection is established over the network and data start passing through it in encrypted form of the onion[5]. finally the data is sent to receiver send by the sender by encrypting at each level of intermediate proxies and finally it decrypted at the initiating proxy and serves as plain text the sender. A.

5.1 Execution Steps: 1. Start Connection.

2. Data Encryption with salt.

3. Key Exchange – Diffie Hellman

4. Network communication using ToR

5. Files Transferred to router

6. Connection End.

Secure and reliable data forwarding using onion protocol This paper proposes onion routing protocol with Advanced Encryption Standard and multi hop route forward algorithm to overcome the existing problems. This system provides a very securable and fast packet transmission in multi hop wireless adhoc network. It provides the reliable and secured packet delivery. In this proposed system based on request response scheme, source selects the path from source to destination node. When ever node registering into the network, it will get node id, primary key, and secondary key. These primary keys and secondary keys are used for encrypting and decrypting the data packets. Once Source discovers the destination, it starts to find shortest path to forward packets. This system uses the multi hop route forwarding algorithm to find the shortest path. After finding shortest path Source collect the primary keys of all intermediate nodes and encrypt the data using that primary keys. This wholesome is forwarded to first node, where first decryption is started using that secondary key. Like that all the intermediate nodes are decrypted. Finally source will get secured and reliable data. B. Node Construction with Communication In this proposed system, first we need to construct the network with n number of nodes. After that nodes can forward data from one to other node in that network. Nodes in the network are moving, because it's having the mobility property.

V. CONCLUSION

Ata security become the most important part in the network building.We shloud need to create such netwrk that provide security in avoiding data mdification and eve dropping in the network.Onion routing with salt make the network more secure and data more protected.To create and provide main aim of onion routing its uses public key encryption with salting method to put multiple layer of encryption around the original data thus making an onion like structure and each layer between source to destination peel off each layer of encryption. As the data reached t the destination it is fully secured as only next router can get address of previous node. So node will ever know the full path of onion. This project resolves the security requirements of unconditional anonymity for honest users and traceability of misbehaving users. Onion wrapping (Wron) and unwrapping (Unwron) methods are central building blocks in onion routing algorithm. In this project have three core properties of onion routing algorithms are focused. The first property is correctness, i.e., if all parties behave honestly, the result is correct. The second property is the security of statefulness, coined synchronicity. It roughly states that whenever a wrapping and unwrapping algorithm are applied to a message with asynchronous states, the output is completely random. The third property is end-to-end integrity.

VI. REFERENCES

[1]. Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[2]. G Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom proposed to generate RSA Public keys and Private Keys for public and private access, 2009.

[3]. Wei Liu: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" , IEEE Transaction on vehicular technology,Vol.63,no.9,November 2014.

[4]. Onion Routing for Resistance to Traffic Analysis by Paul Syverson, 2003, IEEE

[5]. K. Kaviya" Network Security Implementation by Onion Routing" 2009 International Conference on Information and Multimedia Technology.

[6]. Michael Backes,"Provably Secure and Practical Onion Routing", 2012 IEEE 25th Computer Security Foundations Symposium

[7]. Wu and Li S, Khan, Nabil A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks", Computer Networks, vol. 56, no. 2, 2012, pp. 491-503.

[8]. J Ben-Othman,. and Y.I.S. Benitez, "IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s", Concurrency and Computation Practice and Experience, 2011, DOI: 10.1002/cpe.1813.

[9]. Ben-Othman "Achieving Privacy in Mesh Networks", In Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '06), Alexandria, VA, USA, pp. 13-22.

[10]. Benitez M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connections and Onion Routing", IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, 1998, pp. 482 - 494.

[11]. Jin yuan Sun, Member, IEEE, Chi Zhang, Student Member, IEEE, Yanchao Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks". IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 2, MarchApril 2011.

[12]. Chi-Yin Chow, Student Member, IEEE, Mohamed F. Mokbel," A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks" IEEE Transactions On Mobile Computing, Vol. 10, No. 1, Jan 2011.

[13]. David chaum "Blind signatures for untraceable payments" copyright(c) 1998,springer-verlag