www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7850-7856

Data Security for Wireless Mesh Network Using Onion Routing Algorithm

Shruti Patil[1], Suvarna Kanakaraddi[2], Chetankumar Patil[3]
[1] Department of C SE,
[1] B V B College Of Engineering
hubli, India
[2]Department of C SE
[2]B V B College Of Engineering
hubli, India
[3]Dept of E & C
[3] AGMRCET,Hubli,India [3]
Hubli,India

ABSTRACT:
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. Wireless mesh network (WMN) is a new wireless networking paradigm. Unlike traditional wireless networks, WMNs do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. Wireless internet service provider is choosing WMNs to offer Internet connectivity, as it allows a fast, easy and inexpensive network deployment. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we investigate the principal security issues for WMNs. We study the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore approaches to secure its data communication.

[1] INTRODUCTION

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. Also, WMNs are characterized by infrequent topology changes and rare node failures WMNs can be classified depending on the architecture in infrastructure /backbone WMNs. client WMNs and Hybrid WMNs. In infrastructure WMNs mesh clients can join the network only through the mesh routers.

In client WMNs mesh nodes constitute the actual network while in Hybrid WMNs mesh client may join the mesh network either by connected to the mesh backbone or among each other. Figure 1 depicts wireless mesh architecture through the different configurations.

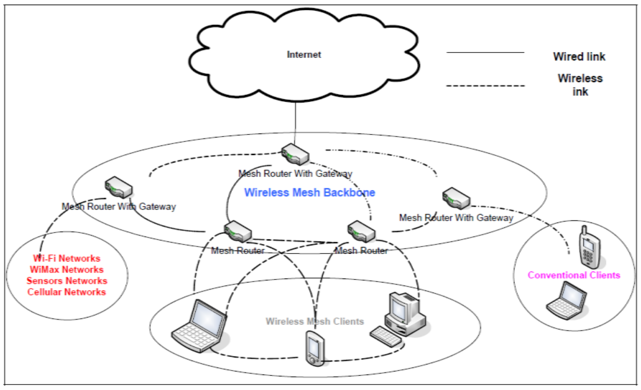


Figure 1: Wireless Mesh Architecture

WMNs can be easily used to build up large scale wireless networks. For that reason, IEEE has established several working groups with aim to develop their mesh standards with coverage ranging from a Personal Area Network (PAN) to a Metropolitan Area Network (MAN), as it can be seen from Table 1.

Types of Mesh Technology	IEEE Specification
WPAN mesh	802.15.5
WLAN mesh	802.11s
WMAN mesh	802.16a, 802.16e, 802.20

Table 1: Types of Mesh Technology

Several companies are developing their proprietary WMN solutions. Foremost performance metrics employed to analyze performance of a WLAN are throughput, packet delivery fraction and end-to-end delay. This analysis is further extended by varying the size of the network so as to obtain the effects on the two performance metrics in security enabled simulated wireless LAN environment with different number of nodes.

[2] LITERATURE SURVEY

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 to the 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.

This paper is motivated by resolving the above security conflicts, namely trace-ability and anonymity in the emerging WMN communication systems. As a result provide detailed efficiency analysis in communication, terms of storage, and computation in this paper to show that our SAT is a practically viable solution to the application scenario of interest. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways. A mesh network is reliable and offers redundancy [13]. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. A Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.15, 802.16, cellular technologies or combinations of more than one type. Wireless mesh network can be seen as a special type of wireless ad-hoc network.

Anonymous routing serves as the enhancement to the user privacy, and we can provide multihop uplink communications among clients in WMN. It is important for the user to be aware of his level of privacy[9]. It makes a system more reliable and trustworthy for the user. Hence the level of the user's anonymous range was fixed by this scheme which entirely monitors the network. There exist certain Time To Live [TTL] value for particularly binded with the ticket's validity which indicate the time period for the service for that session. If the user exceeds the TTL value the system excludes the user from the network.

Communication systems, it is easier for a global observer to mount traffic analysis attacks by following the packet forwarding path than in wired networks[10]. As a result, the original anonymity scheme for payment systems among bank, customer, and store cannot be directly applied. 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. Moreover, although employ the widely used pseudonym approach to ensure network [12].

It refers to the property that multiple packets cannot be linked to have client. For instance, if the network ID (i.e., IP address, MAC address) of a client's device is fixed and exposed in packet forwarding, the packets sent by a same client can be linked, which will enable the attackers to profile the client through traffic analysis attacks.

[3] 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 2: 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

[5] RSA ALGORITHM STEPS:

Steps1: Key generation: whoever wants to receive secret messages creates a public key (which is published) n a private (kept secret).the keys r generated in a way that conceals their constructions n make it ‘difficult’ to find private key by only knowing public key.

Step 2: Encryption: a secret message to any person can be encrypted by his o her public key (that could be officially listed like ph no).

Step 3: Decryption only the person being addressed can easily decrypt the secret message using private key.

In this paper, we embed an efficient asymmetric encryption strategy to protect and ensure anonymity for source routes when employing a source routing protocol. The base protocol used for source routing is DSR and to prevent DOS attack which occurs by converting the data into ASCII word and then modifying data by wrapping and unwrapping so that allow transmission of data. Then respective symmetric key is used to encrypt & decrypt the transmission. Each connection of onion router is implemented using linked list. Each data fetched is attached to the tail of list.

We identify the onion wrapping (Wron) and unwrapping (Unwron) algorithms as central building blocks in onion routing. We identify four core properties of onion algorithms. The first property is correctness, i.e., if all parties behave honestly, the result is correct. The second property is the security of state fullness, 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. The fourth property states that for all modifications to an onion the resulting changes in the cipher text are predictable.

6. RESULTS

Here is the comparison of different algorithm with the parameters and Secure Onion Routing Algorithm will give best result in identifying shortest path in wireless mesh networks.

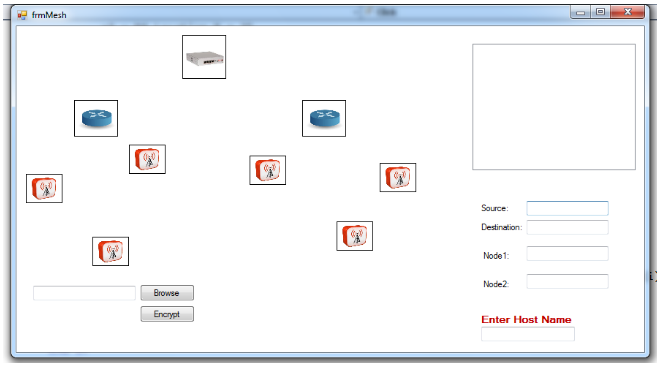
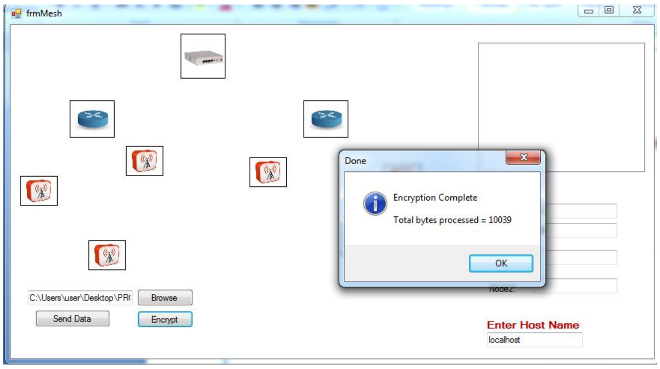


Figure 6.1: Initial setup of the network

Initial setup of the network with 9 nodes. User can enter the source and destination where they can send the data. User should enter host name to send file.



Encryption Complete

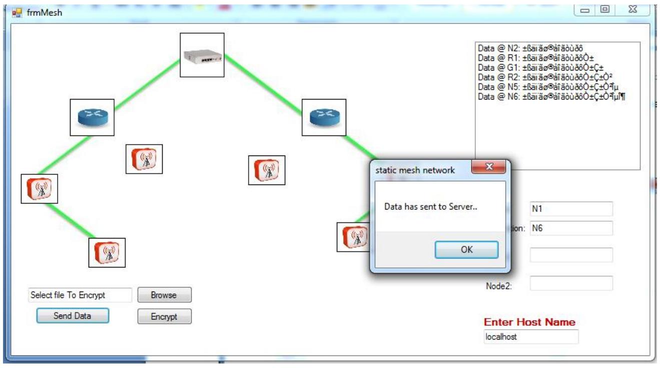
Total bytes processed = 10039

C:\Users\user\Desktop\PR(

localhost

Figure 6.2: Encrypted data at client

Here data is browsed and encrypted and can view size of the file encrypted in bites at client.



```
Data @ N2: ±ßaïãø®åîãòùðô
Data @ R1: ±ßaïãø®åîãòùðôÒ±
Data @ G1: ±ßaïãø®åîãòùðôÒ±Ç±
Data @ R2: ±ßaïãø®åîãòùðôÒ±Ç±Ò²
Data @ N5: ±ßaïãø®åîãòùðôÒ±Ç±Ò¶µ
Data @ N6: ±ßaïãø®åîãòùðôÒ±Ç±Ò¶µÎ¶
```

Data has sent to Server..

Select file To Encrypt

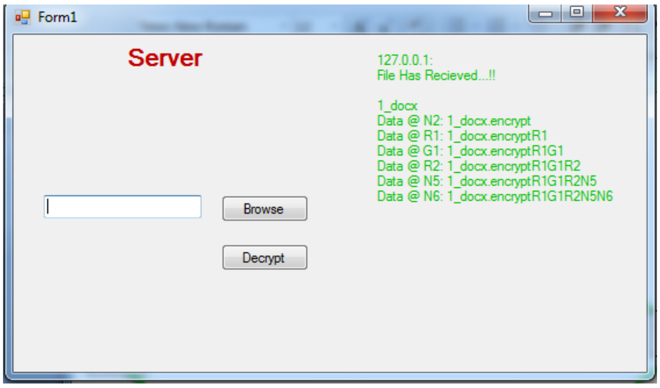
N1

N6

localhost

Figure 6.3: Data wrapped at client

Here file is encrypted and wrapped at client side and data is sent to server.

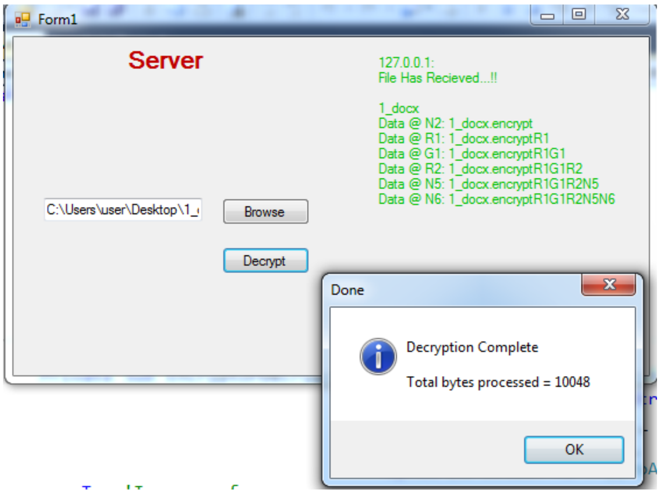


```
127.0.0.1:
File Has Recieved...!!

1_docx
Data @ N2: 1_docx.encrypt
Data @ R1: 1_docx.encryptR1
Data @ G1: 1_docx.encryptR1G1
Data @ R2: 1_docx.encryptR1G1R2
Data @ N5: 1_docx.encryptR1G1R2N5
Data @ N6: 1_docx.encryptR1G1R2N5N6
```

Figure 6.4:Data unwrapped at server

Here file is unwrapped at client side and view the client IP address.



```
127.0.0.1:
File Has Recieved...!!

1_docx
Data @ N2: 1_docx.encrypt
Data @ R1: 1_docx.encryptR1
Data @ G1: 1_docx.encryptR1G1
Data @ R2: 1_docx.encryptR1G1R2
Data @ N5: 1_docx.encryptR1G1R2N5
Data @ N6: 1_docx.encryptR1G1R2N5N6
```

Decryption Complete

Total bytes processed = 10048

Figure 6.5: Decrypted data at server

Here file is unwrapped at server side and view the client IP address, and after decryption can view the decrypted file size.

7. CONCLUSION

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.

By analyzing the characteristics of WMNs and have deduced two fundamental network operations that need to be secured for data transmission: (i) use of a secure routing protocol, and (ii) enforcement of a proper fairness in data transfer. In this project we have proposed solutions to secure the data transfer by using onion routing algorithm and RSA cryptographic algorithm for data security.

8. FUTURE WORK

- This project can be enhanced for dynamic architecture.
- Size of data can also be increased which improves performance.
- Increase in wrapping layers improves security.
- Each layer there should be wrapping and unwrapping.

REFERENCE

[1]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.

[2] 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.

[3] 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.

[4] 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.

[5] 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, March-April 2011.

[6] 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.

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

[8] Steve Glass ,Marius Portman ,"Securing wireless mesh networks" Published by the IEEE Computer Society 1089-7801/08/$25.00 ©2008 IEEE.

[9] Taojan Wu, Yuan Xue "preserving Traffic Privacy in Wireless Mesh Networks" Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks

[10] Yalin Chen Jue-Sam Chou "A novel electronic cash system with trustee-based anonymity revocation from pairing" 1567- 4223/$ - see front matter _ 2011 Elsevier .

[11] Yanfei Fan, Yixin Jiang, Haojin Zhu, Member, IEEE, Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks" IEEE Transactions On Wireless Communications, Vol. 1 0, No. 3, March 2011.

[12] Mr. M.A.Baseer AND Mr. Bhusari Dipak Govardhan SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks International Journal of Innovative Technologies, Vol. 01, Issue 02, Sep 2013.

[13] M.Jayanthi and .M.A.Mukunthan International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-ETIC-2011, January 2012 A Security Architecture for Implementing Anonymity and Traceability In Wireless Mesh Network using Clustering Concept.

Shruti Patil

Mtech , BVBCET ,Hubli
Presented National Conference On Near Field Communication Using Smart Phone

SUVARNA.KANAKARADDI
Currently working in BVBCET,Hubli
Associate professor
15 YEARS OF EXPERIENCE

Chetan Patil

3 years teaching experience
1 year industrial experience on embedded system

Corresponding Address-

SHRUTI PATIL
D/O DR.P.R.PATIL
PRABHU NURSING HOME
TQ:SHIGGAON
D:HAVERI
Pin code :581205