International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 4, April-2014, pp: (115-120), Impact Factor: 1.252, Available online at: www.erpublications.com

A policy enforcing mechanism in trusted Wi-Fi network and Stepping Stone Detection

Prakash Munde[1], Rupesh Pokharkar[2], Tejashri Jagtap[3]
[123]Department of Computer, Parvatibai Genba Moze College of Engineering,
Wagholi, Pune, Maharashtra, India

Abstract: Wi-Fi network is network which can connect two or more node on basis using access point. Problem associated in Wi-Fi network are eavesdropping attack, active attack, file sharing problem , unauthorized accesses of server and malicious activity on server, web problem and routing protocols problem. Using Wi-Fi technology limitation of Wi-Fi network are remove but until scope of technology is very wide, we can create trusted Wi-Fi network using hotspot and share internet access on one node to multiple node. Problem of Wi-Fi network are solve using trusted network ,secure file sharing, server monitoring and stepping stone using watermarking technique. Using above technique to solve Wi-Fi network problem and increase throughput of system in the network and also provide security from unauthorized access and different harmful activity.

Keywords: Trusted Network, Secure File Sharing, Policy Enforcing.

I. INTRODUCTION

Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting messages, injecting erroneous messages, impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Protect the servers from unauthorized client accesses. In wireless , this distinction does not exist as every node can be a server and a client at the same time, and no entity can be trusted more than another. Newer Wi-Fi technology eliminates many of the ad hoc wireless network limitations and is more secure, but until that technology is more widespread, you can Set Up an Ad Hoc Wireless Network and use it to Share Internet Access on one computer to many devices.

Fig 1: Wi-Fi ad hoc mode Network

Ad hoc networks are useful when you need to share files or other data directly with another computer but don't have access to a wireless network .You can also use Internet connection sharing with ad hoc mode to share your Internet connection with other users. Another feature of ad hoc networks is that more than one laptop can be connected to the ad hoc network, as long as all of the adapter cards are configured for ad hoc mode and connect to the same SSID (service state identifier). The computers need to be within 100 meters of each other. Also, if you were the person who set up the ad hoc network, when you disconnect from the network, all of the other users will also be disconnected. An ad hoc network will also be deleted once everyone on it disconnects which can be good or bad, depending on your view; it's truly a spontaneous network.

Problem associated in wireless ad hoc network are eavesdropping attack, active attack, file sharing problem , unauthorized accesses of server and malicious activity on server, Internet Connection Sharing problem and Ad-hoc routing protocols problem. Using Wi-Fi technology limitation of wireless ad hoc network are remove but until scope of technology is very wide, we can create ad hoc network using hotspot and share internet access on one node to multiple node. Problem of wireless ad hoc network are solve using trusted network ,secure file sharing and stepping stone. Using above technique we can solve wireless ad hoc network problem and increase throughput of system in the network and also provide security from unauthorized access and different harmful activity. We can create ad hoc network using hotspot and share internet access on one node to multiple node. Problem of wireless ad hoc network are solve using trusted network ,secure file sharing and stepping stone. We can solve wireless ad hoc network problem and increase throughput of system in the network and also provide security from unauthorized access and different harmful activity.

II. LITERATURE SURVEY

A. EXISTING SYSTEM WORK

The communications between all nodes in the network by enforcing a unified group policy on a set of middleware controllers. However, The controllers to be trusted, but does not provide means of establishing the trust. Consequently, in practice, it can only be applicable in controlled environments where the enforcers can be deployed , such as corporate intranet and Internet P2P. Another step by developing a shared trusted reference monitor across a coalition of nodes using remote attestation. Enforces communication policies at the virtual machine level and requires that each node runs multiple virtual machines , which may not be practical for mobile devices. Additionally, does not provide enough flexibility to compose applications and policies. If an application depends on others, then all of them together with their policies must be isolated in one virtual machine. Different than enforcing policies in the network, another approach is to allow only nodes owned by trusted principals to participate in the network.

The method does not address the case of anonymous nodes spontaneously establishing ad hoc. Furthermore, such methods provide insufficient level of security because a known-to-be-trusted node is more likely to be compromised and taken over by an attacker in ad hoc than in infrastructure based networks, due to the lack of physical protection. The design and implementation of a policy enforcing mechanism based on a kernel-level trusted execution monitor. Under this mechanism, each application or protocol has its own policy All nodes supporting a certain application and enforcing its policy form a trusted application- centric network. Since an application may depend on other applications, our policy enforcing mechanism creates a trusted multi-tier network. The member nodes in such a network must enforce the policies associated with these applications as well. For instance, a peer-to-peer file sharing application may depend on an on-demand routing protocol. In this case, the mechanism creates a two-tier trusted file sharing network. It first establishes a trusted routing tier, and hence a trusted network for routing, comprising of all the nodes that enforce the routing policy. On top of this tier, it then creates a file sharing tier, enforcing the file sharing policy. In our policy enforcing mechanism, nodes can be members of multiple multi-tier networks simultaneously. Two nodes may communicate through an application if and only if they enforce the same application tier policy and all the underlying tier policies.

B. ISSUES WITH EXISTING SYSTEM

- Less security to data transmission
- No trust between communication.
- Active attack
- Lack the infrastructure
- Problem of stepping stone

III. PRAPOSED SYSTEM MODELS

For above mentioned problems with the existing system we are developing the formulated solutions to remove these problems.

1. Creation of Trusted Wi-Fi network

Firstly initiator (server) initiates the communication using Wi-Fi ad hoc mode type of network. Whenever user want to communicate to the our Wi-Fi Network then authentication of user is required to make trust between number of user. So

that's reason implement the concept of Password generation or initial key generation or one time password. User or client enter into network when he has secrete key which is given by server at the time of registration of client and time of client want to service from server. This key(password) only valid for one session, next time client request to server then assign new key for this session. This password generated using combination of the color and cube surface, take the color coordinator like red, green, blue value and sequence of the color.

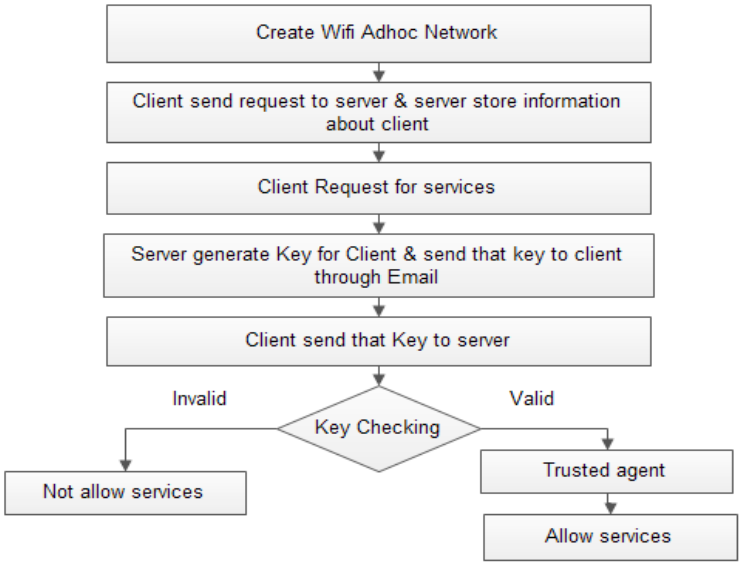

Fig 2: Flow Diagram of creation of trusted Network

Using hybrid color authentication scheme we generate the Password as per above mentioned, so the following diagram show the password generation.

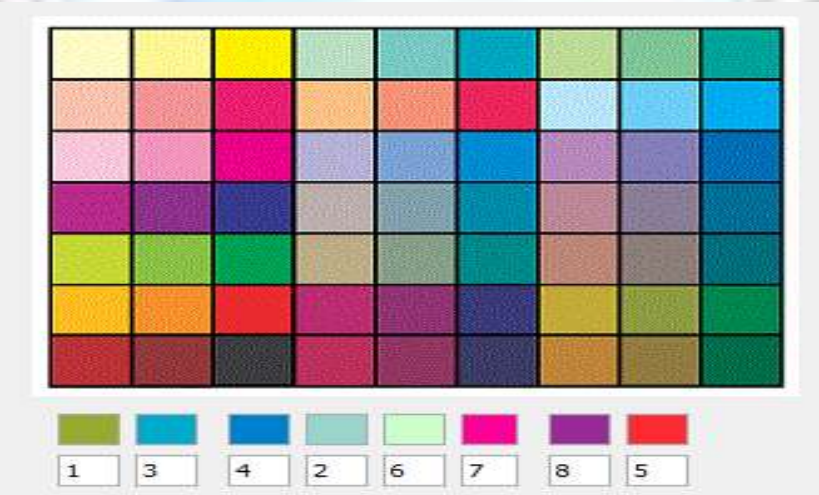

Fig 3: Color scheme for password generation

2. Policy Enforcement

"Policy Enforcement" in the context where we want to control access to a network. Why use this? Because you can control access to your network in the event of a problem. If a new virus starts to propagate across your network, or if a user brings a laptop computer into the network from the outside that has inappropriate software, No longer do you have to simply allow any random machine to connect to the network. This can significantly improve the defense of the network. "Network Policy Enforcement" is the application of some sort of network access control mechanism to control access to a network. The criteria for whether an end system is allowed to access the network are specified in a set of rules or parameters known as a "policy". Using a Policy Enforcement Point, make a decision regarding which parts of the network, if any, that the device should be allowed to access.

3. Secure File Sharing

A peer-to-peer file sharing application may depend on trusted network. In this case, the mechanism creates a trusted routing tier, and hence a trusted network for routing, comprising of all the nodes that enforce the routing policy. On top of this tier, it then creates a file sharing tier, enforcing the file sharing policy. In our policy enforcing mechanism, nodes can be members of multiple multi-tier networks simultaneously. After creation of trusted network data of file is encrypted and send that encrypted data to its destination .in this way we can security during data transmission.

In following fig a tier is created step-by-step. First, a node begins to enforce the tier policy. It creates the tier key, which is used to authenticate in tier communications. By doing so, it becomes the first member of the tier, called originator of the tier, e.g. node 1. The originator then broadcasts an invitation to its neighbors, e.g. node 3 ,node4 and node5, to join the newly created tier. Assume node 2 not part of trusted network .After successful creation of trusted network node 1,node 3 ,node4 and node 5 perform secure file sharing application but node 2 cannot share file in network because node2 is not part of trusted network.

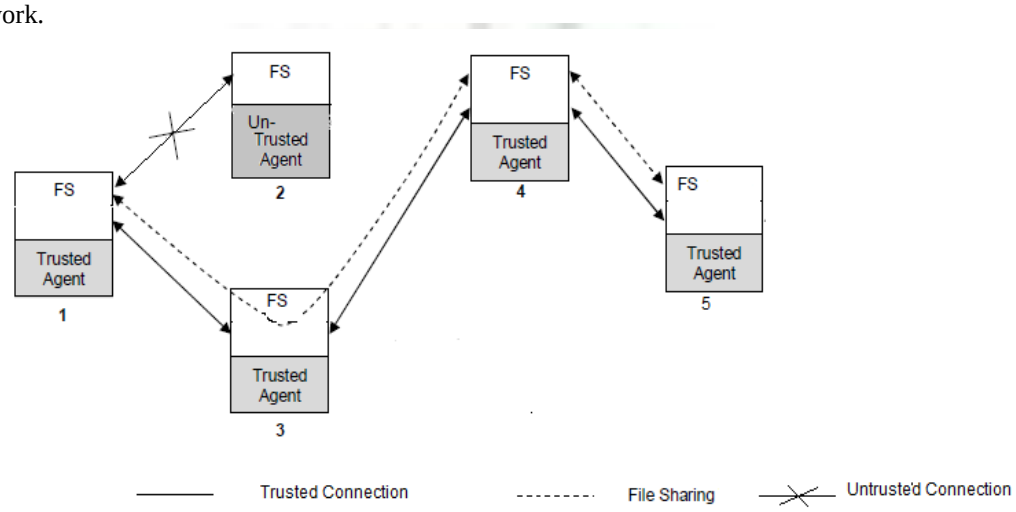

Fig 4: Trusted File Sharing

3.1 AES Algorithm for File Sharing

AES(Advanced Encryption Standard) is symmetric key block cipher cryptographic algorithm which is used for the provide the confidentiality for the information.AES uses the 128 bit block size for encryption/decryption like operation and also 128 bit key is use 10 rounds,192 bit uses 12 rounds, and 256 bit uses 14 rounds.AES performs the following functions: • SubBytes() • ShiftRows() • MixColumns() • AddRoundKey() The first three functions of an AES round are designed the methods of confusion and diffusion. The fourth function actually encrypts the data. These we may call the methods of diffusion and confusion. Diffusion means patterns in the plaintext are dispersed in the cipher text. Confusion means the relationship between the plaintext and the cipher text is obscured. SubBytes adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm. Arranges the state in a matrix and then performs a circular shift for each row. This is not a bit wise shift. The circular shift just moves each byte one space over. Each of the 16 bytes of the state is XORed against each of the 16 bytes of a portion of the expanded key for the current round. The Expanded Key bytes are never reused.

3.1.2 Diffie–Hellman

It is not encryption algorithm but protocol for exchanging secrete key (symmetric key) to be used for sending encryption transmission between users using data encryption standard. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. Diffie–Hellman key agreement itself is an non-authenticated key-agreement protocol, it provides variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's.

1. User1 and User2 agree on two large prime number n & g.This two integer need not kept secret. User1 and User2 use a insecure channel to agree on them. condition[n>g].
2. User1 chooses another one large random number x and calculate, $A=g^x \bmod n$ ……..0 <= x <= n-1.

3. User1 send number A to User2.
4. User2 select independently chooses another large random integer number y and calculate $B=g^y$ mod n ……..0<= y <= n-1.
5. User2 send number B to user1.
6. User1 now calculate secrete key k1.
   $k1=B^x$ mod n.
7. User2 calculate the secrete key k2.

$k2=A^y$ mod n.
k1=k2=k is the symmetric key which User1 and User2 kept secret.
k is symmetric key for session.

STEPPING STONE DETECTION

When unauthorized client hide its own identity and upload some malicious data on web that time we identify such client and block that client .In stepping stone detection system we use water marking technic. when any client upload data our any web that time we take his/her system IP and MAC address automatically store it on sever. If server found any file malicious then server check file details retrieve information related to that file ,remove that file from server and block that client.

WORKING DIAGRAM

Create ad hoc network using Wi-Fi technology. Apply different read/write Policy(policy Enforcing) to different client for creation of trusted network. After successfully creation of trusted network provide session key to each user when it send request for file sharing or chatting. We use AES algorithm for secure file sharing and we prevent fake account chatting using trusted agent concept.

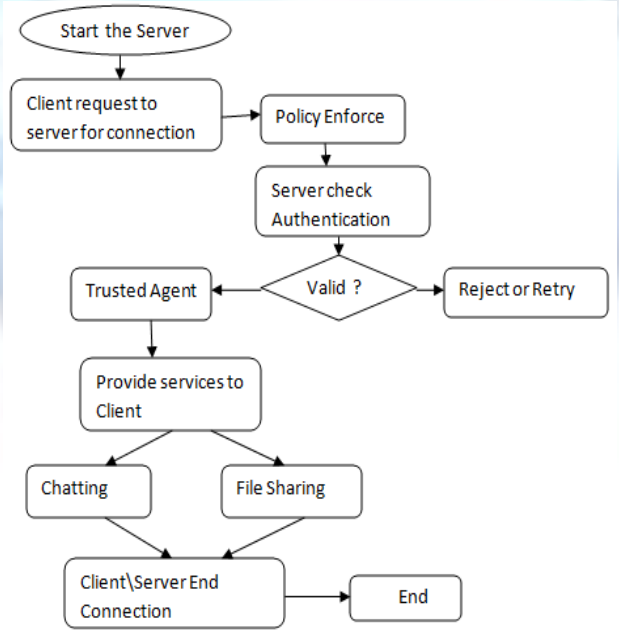

Fig 5: Working Diagram

APPLICATION

1. Home and enterprise networking: Conferences, meeting rooms ,Personal area networks (PAN), Personal networks (PN) and Networks at construction sites.
2. Education : Universities and campus settings ,Ad hoc communications during meetings or lectures
3. Entertainment: Multi-user games , Wireless P2P networking, Robotic pets
4. Coverage extension: Extending cellular network access
5. Tactical networks: Military communication and operations

6. Commercial and civilian environments

ADVANTAGES

Secure File Sharing

Creation of trusted network data of file is encrypted and send that encrypted data to its destination .in this way we can security during data transmission.

Avoid unauthorized access

Using stepping stone we can avoid unauthorized client enter into system.

Increase throughput

We can solve wireless ad hoc network problem and increase throughput of system in the network and also provide security from unauthorized access and different harmful activity

FUTURE SCOPE

We can use this concept in company, college campus or any private or public area creation of secure wireless network. Scope of project increases when we use wi-max instead of Wi-Fi. Using Wi-max create wireless network and we can cover large distance of campus or area. To transfer the data with security goals like Authentication, confidentiality we enhance the existing algorithm with different one. In Military communication we use this particular concept.

CONCLUSION

In this paper we introduce the concept, basically done the literature survey briefly. Also done the study of various problem and its formulated solutions. Using above mentioned technique we can provide the security to the application of the Wi-Fi network efficiently. To overcome the drawbacks of the Wireless network, we use the formulated solutions such as secure file sharing, stepping stone detection, sever monitoring, encryption/decryption technique.

REFERENCES

[1]. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in the Proceedings of IEEE Conference on Privacy and Security, 1996, pp. 164–173.
[2]. S. Capkun, J. Hubaux, and L. utty´an, "Mobility helps security in ad hoc networks," in the Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), June 2003, pp. 46–5.
[3]. G. Xu, C. Borcea, and L. Iftode, "Trusted application-centric ad-hoc networks," in the Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc Networks and Sensor Systems (MASS 2007), 2007.
[4]. R. Merkle, "Secure communication over an insecure channel," submitted to Communications of the ACM.
[5]. Y. Zhang and V. Paxson, "Detecting stepping stones," in In Proceedings of the 9th USENIX Security Symposium, 2000, pp. 171–184.
[6]. L. Adleman, A subexponential algorithm for the discrete logarithm problem with application to cryptography, Proceedings IEEE 20th annual symposium on foundations of computer sci- ence, 1979, pp. 55–60.
[7]. R.Dhamija and A.Perrig."Déjà vu:A User Study Using Images for Authentication".In 9th USENIX Security Symposium,2000.
[8]. Cox, I., Miller, M. L., and Bloom, J. A. (2002). Digital Watermarking. Morgan Kauf- mann.
[9]. T. Woo and S. Lam, "A framework for distributed authorization," in the Proceedings of the 1st ACM Conference on Computer and Communications Security, November 1993, pp. 112–118.