International Journal of Engineering & Technology, 7 (2.4) (2018) 200-203

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Four-way handshake protocol for authenticating in multiple mix-zones

T. Senthil Kumar [1] *, S. Prabhakaran [1], V Prashanth [1]

[1] CSE Dept., SRM Institute of science & technology, Chennai, Tamil Nadu
**Corresponding author E-mail: Senthilkumar.t@ktr.srmuniv.ac.in*

Abstract

Authentication is the process of verifying that the users who they claim to be or not, it is based on identity and credentials. Most of the attacks can be reduced using authentication process. Authentication is important because as the amount of online data sharing has increased, threats and fraud in a large amount are also increased, a changing of the guard which provides security to mobile devices is needed for which authentication is necessary. Privacy of user's location is important in mobile networks, there are several strategies to protect the personal information (i.e., their location). In previous work it is introduced that the mix zone model which will change the old pseudonyms to new pseudonyms and anonymizes user's identity by restricting the position where users can be located. Later work, even in the multiple mix-zones model, attackers can attack by using side information (like footprints, navigation etc.). So, we need an authentication protocol while two mix-zones or user-services are communicating. We came across different authentication protocols like PAP, CHAP, and EAP. In this paper, a four-way handshake protocol is implemented for providing authentication while multiple mix-zones are communicating. A four-way handshake authentication protocol i.e., WPA-PSK protocol for verification. WPA-PSK is applied in such a way that both STA(supplicant) and AP(authenticator) can check that they are re-agreeing on a non-forged RSN and IE, therefore they are using the most secure available protocols.

Keywords: *Authentication; Mobile Networks; Loca--Tion Based Service; Mix-Zone; Four-Way Handshake.*

1. Introduction

When we are implementing a wireless module, we must keep security, power consumption, Interference and Reliability in required state. with all this constrains we can improve the privacy of mobile stations in the LBS by using Mix-Zone model. Location based Service (or LBS) is a customized benefit that depends on the area of a versatile data gadget client. If there should be an occurrence of business as a vehicle following gadget or resource following part, LBS innovation goes about as an impetus in the development of enterprises particularly media transmission and transportation. Area security is an essential new issue and a few systems that is used to secure individual area data. In past work it is presented that the mix zone display anonymizes client personality by confining the positions where clients can be found.

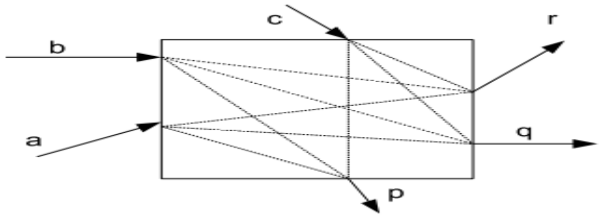


Fig. 1: Mix Zone Model.

Let's consider a mix zone with k number of people and the people are traveling in certain area where the mix-zone is allocated. When the mobile devices are travelling from that mix-zone area the unique identity reference numbers which are used to track will get changed. In a simple word it will change their old pseudonym (Eg: Actual Location of the mobile station) to the New pseudonym (dummy Location) and by this we can understand that mix-zone will take the actual location of the user and change that location to the dummy location so that the actual location of the user is hidden. By this we can increase the privacy of the user's data in the geographical area. If we want to preserve the location of user's while travelling from one location to other location and when we implement the mix-zone model in any access point the working of that mix-zone is shown in figure their we can observe that location names with a, b and c are changed to p, q and r when the mobile stations are passed through the mix-zone area. By this we can improve the privacy of user's location. Here, there are chances of reveling over information by the side information like navigation and any location reveling applications. This case will arise when multiple mix-zones are used. We go for multiple mix-zones to increase the privacy of user's data. So, we are implementing a secured authentication protocol between two mix-zones. Here, we are implementing a four-way handshake protocol to authenticate two mix-zones before they exchange the key.

2. Related works

According to Wei Xi & Chen Qian, they worked on paring algorithm in which they used to reduce the harder problem in one group and easier one in another group. To solve the problem, they used Max-Weighted Bi- partite Matching in parsing algorithm. it collects every one of the highlights separated from G0 and G1 into two sets C0f and C1f to speak to 0 and 1 bits individually. The above issue can be formalized as a Max-Weighted Bipartite

Matching issue. At that point it illuminated by use Kuhn-Munkras calculation and guide the 0 and 1 bits to the highlights. [3] According to Jinsong Han & Kun Zhao, KM based feature pairing algorithm, in this we will generate maximum match graphs. For every pair the deference will be less than 9(where it is greater then 5). we will establish that KM algorithm is constant, i.e., the remaining graph not including minimal edge is also a maximum match are found in the graph. Before discarding to M it will denote maximum weights of graph G, and it will maximum weight after to be M, and it will maximum weight after discarding edge ei',j', named GL, to be M-W(ei',j'). [4].

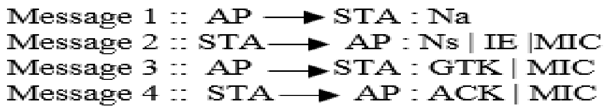
Mustafa AL-Fayoumi proposed that Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A confirmation system is a procedure intended to enable all members to demonstrate their lawfulness and check the other member's characters that engaged with the systems. This instrument utilizing mystery key K, then if we take cryptographic calculations - incorporate there will be three message validation codes like f1, f1*and f2 and four key age capacities f3, f4, f5 and f5* are shared amongst HLR/AuC and MS. That is known as confirmation and key assertion convention (AKA). The AuC keeps up a counter called grouping number (SQNHLR), where client MS keeps up a counter (SQNMS), whose underlying incentive for these counters are set to zeros. [5].

According to Jafer AL-Saraireh, to moderate the calculation weight of portable hardware, the encryption is clone in MS side since the general population key activity takes O (K2) unpredictability however private key task takes O (K3) multifaceted nature with the commonplace secluded exponentiation calculations used to execute the RSA calculation, where K is the quantity of bits in the modulus. The product paces of RSA are said. In view of the e esteem the RSA can work much faster.in that work he pick e as littlest esteem. To make utilization of open key cryptography on the low calculation versatile hardware, the insignificant key length for general information is 1024 bits. NIST has suggests 1024 bits for RSA, which is thinking about the lifetime of the information. For security concerns and the execution rates of the general population key encryption, they recommended estimation of open key length is ideally 1024 bits. [6].

According to SK Hafizul Islam, Polynomial Time calculation is said to be reasonable in polynomial time if the quantity of steps required to finish the calculation for a given info is for some nonnegative number, where is the multifaceted nature of the information. Polynomial-time calculations are said to be "fast." Given two random elements $(P, aP, bP) \in G_p$, for any polynomial time algorithm it is computationally hard to find the integer $a, b \in_R Z_p^*$, such that Q ¼ aP. Polynomial-time limited calculation is computationally infeasible. What's more, a 160-piece measure ECC-based key offers an indistinguishable level of security from that got utilizing a 1024-piece RSA-based key. Further, the rudimentary tasks like point augmentation, expansion and so forth in the elliptic bend aggregate are substantially quicker than the secluded exponentiation executed in the multiplicative gathering. Along these lines, the ECC-based conventions are productive as far as (1) security, (2) calculation, (3) stockpiling and (4) correspondence data transfer capacity. Computational Diffie– Hellman here the problem $(P, aP, bP) \in G_p$ for any $a, b \in_R Z_p^*$, they gave random instance and computation of abP is infeasible by this algorithm. [7]

3. Proposed work

we are implementing a four-way authentication protocol in which each mix zone will authenticate before connecting to other mix-zones. In four-way authentication protocol when data is transferring between multiple mix-zones. A WPA-PSK protocol which is also called four-way handshake authentication protocol is used for verification of mix-zones when two mix-zones are communicating. There is a need to provide the security to avoid several attacks. In day to day life the as the communication become easy and the data transfer through wireless is increased so there is a need to increase the security to the data while transferring. A four-way handshake which is used to confirm the STA know as secret Pre-Shared Key and the other name of secret pre-Shared key is Pair Wise Master Key (PMK), and for transmission purpose To establish a Pair Wise Transient Key (PTK) which is installed into the MAC layer we will be using PTK.so that the key will be hidden.


Message 1 :: AP ⟶ STA : Na
Message 2 :: STA⟶ AP : Ns | IE |MIC
Message 3 :: AP ⟶STA : GTK | MIC
Message 4 :: STA⟶ AP : ACK | MIC

Fundamental objective of WPA-PSK convention is producing a PTK known both to STA and AP where we won't uncover the PMK. To begin with, according to four-way handshake protocol the PMK is arbitrarily created by STA, encoded and directed to the confirming AP. Together AP and STA will along these lines have the capacity to achieve a PTK from PMK. Afterward an effective 4-Way Handshake, a protected correspondence channel between the authenticator and the supplicant can be developed for ensuing information transmissions, in view of the mutual PTK. Same process is rehashed by utilizing the same PMK. the STA and AP is MAC areas and two 32 byte long subjective delivered by STA and AP called SNonce and ANonce.by this we can improve the assurance of the Mobile stations while two mix zones are affirming.

3.1. Modelling of WPA-PSK in mix-zone

Initially, we must create a system with mobile nodes, Access Points, Nodes for communication (packet transfer) between mobile station's, nodes, access points. The system set up contains various modules which are explained below.

1) Wlan Deployment
2) Encryption
3) Data Communication
4) Wpa_Psk
5) Decryption

1) WLAN Network Deployment

The beginning stage in a remote LAN (WLAN) association is to ensure that desired assignment begins with a site outline to study the Radio Frequency (RF) lead in a space. Various issues can develop in a remote framework due to absence of prescience and degree. It has been found that numerous site reviews are not performed legitimately or the site study is excluded inside and out. The expected motivation behind this archive is to give rules to legitimate arranging, readiness, and distinguishing proof of the key things to check through the investigation of an overview report. WLAN is made from a few remote hubs, every one of which screens ecological characteristics, records detecting information, infers natural conditions by collecting the detecting information, and returns the totaled information to the Access Point.

2) Encryption:

RSA is a calculation utilized by present day PCs to scramble and decode messages. It is an awry cryptographic calculation. Hilter kilter implies that there are two diverse keys. This is additionally called open key cryptography since one of them can be given to everybody. The other key must be kept private. It depends on the way that finding the variables of a whole number is hard. A client of RSA makes and after that distributes the result of two expansive prime numbers, alongside an assistant esteem, as their open key. The prime components must be kept mystery. Anybody can utilize people in general key to scramble a message, however with at present distributed techniques, if the general population key is sufficiently extensive, just somebody with information of the prime elements can plausibly unravel the message.

$$c = m^e \mod n$$

3) Data Communication:

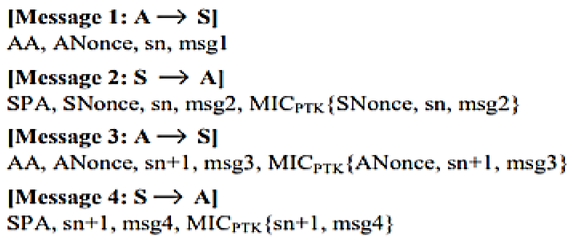
This Module is produced to WLAN systems information correspondence & collection process. The radio & IEEE 802.11 MAC layer representations were utilized. The system originated information handling or costly and information correspondence level on their execution on the system. Numerous bases make and end sending bundles. In our execution, every datum has an enduring size of 512 bytes. Every Sensor hub to move haphazardly on their system, it be increasingly and most fit on their systems.

4) WPA-PSK protocol:

This protocol which is also called four-way handshake authentication protocol is used to verification of mix-zones when two mix-zones are communicating. There is a need to provide the security to avoid several attacks. in day to day life the as the communication become easy and the data transfer through wireless is increased so there is a need to increase the security to the data while transferring. WPA-PSK is also known as four-way handshake which is used to confirm the STA know as Secret Pre-Shared Key and other name is Pair Wise Master Key (PMK), and for transmission purpose we use PTK and this is used to found a Pair Wise Transient Key (PTK) which is mounted into the MAC layer.

Four-way handshake utilizes a pass key called Pairwise Master Key (PMK), and connection of different information things to set up the encryption of information. These incorporate single-utilize things called ANonce and SNonce, and also the Mac locations of the two endpoints included. The principle procedures of the four-way handshake are done to empower an entrance point to validate itself to the customer, and to give secure encryption. The PMK is for the most part not sent over the system, leaving this segment unshared and hence fortifying the security of the procedure.

While there is some level headed discussion about the particular purposes of four-way handshake confirmation, it is utilized to send messages between an entrance point and a customer secure. This mind boggling setup takes into consideration a more secure validation process that matches the multifaceted nature and vulnerabilities of present day systems. Once a mutual PMK is settled upon between the authenticator and the supplicant, the authenticator may start a 4-Way Handshake self-ruling from some other individual or upon asking for from the supplicant. The message trade is appeared, at a dynamic level.



[Message 1: A ⟶ S]
AA, ANonce, sn, msg1

[Message 2: S ⟶ A]
SPA, SNonce, sn, msg2, $\mathrm{MIC}_{\mathrm{PTK}}$\{SNonce, sn, msg2\}

[Message 3: A ⟶ S]
AA, ANonce, sn+1, msg3, $\mathrm{MIC}_{\mathrm{PTK}}$\{ANonce, sn+1, msg3\}

[Message 4: S ⟶ A]
SPA, sn+1, msg4, $\mathrm{MIC}_{\mathrm{PTK}}$\{sn+1, msg4\}

Message. 1: In the First Message, Where it is Forwarded by the Authenticator and Holds the Authenticator Subjective Nonce. Presently, it is not A Scrambled One and There Is No MIC is joined.

Message 2: At that point, the next message is forwarded as a response to first message by the supplicant to authenticator which contains STA sporadic nonce and it also knows every one of the information required to get PTK from PMK. In WPA-PSK the rightness of IE is patterned through MIC affirmation.

Message 3: In the wake of tolerating the second message AP can construe PTK, and then it will be checked to MIC rightness & continue with confirmation by appending GTK in previous message.

Message 4: At that point, the fourth message is a like an assertion sent by supplicant to the authenticator, it contains just a MIC.

The PTK is gotten from the mutual PMK through a Pseudo Arbitrary Function with yield length X (PRF-X), say, PTK = PRF-X (PMK, "Pairwise key extension" || Min{AA, SPA} || Max{AA, SPA} || Min{ANonce, SNonce} || Max{ANonce, SNonce}), and isolated into KCK (Key Confirmation Key), KEK (Key Encryption Key) and TK (Temporary Key). we don't recognize them here in light of the fact that this appears to be inconsequential to the verification procedure.

5) Decryption:

Before we go and decode these messages, it is critical to comprehend that you need to legitimately catch "4-way handshake messages" in your sniffer keeping in mind the end goal to unscramble utilizing wireshark. chance that if you are not catch messages effectively, wireshark won't have the capacity to determine all the keys to decode rest of that information. Here is one illustration where every one of the edges has not been caught legitimately in 4-way handshake process. presently you will be ready to see the movement inside these information outlines. Here is a similar edge (103) which you saw prior in scrambled arrangement, yet now Wireshark ready to unscramble it.

$$m^{ed} \equiv m \pmod{pq}.$$

Thus,

$$c^{d} \equiv m \pmod{n}.$$

4. Results and analysis

The creation of nodes, access points and mobile node are shown in figure. Each mix-zone Contains an Access Point. We created two mix-zones with two Access Points (AP). It shows data transfer between two Access Points (AP), when a mobile node (MN) is moving in that region. As per the module description the model is implemented and we calculated the time taken to generate the key, bit error rate and throughput. The result graphs are shown below.

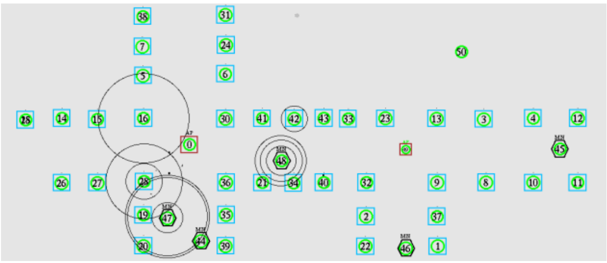


Fig. 2: Node, AP’s, MN’s Creation in NAM.

This module is developed and performance based result analysis of key generation time, packet delivery ratio, bit error rate, throughput ratio is determined.

4.1. Key generation time taken analysis

Key generation is the way of producing keys in cryptography. A key is used to scramble and translate whatever data is being encoded/unscrambled. Exhibit day cryptographic structures consolidate symmetric-key computations, (for instance, DES and AES) and open key figuring’s, (for instance, RSA). Symmetric-key estimations use a single shared key; keeping data secret requires keeping this key riddle. Open key figuring’s use an open key and a private key. General society key is made available to anyone (habitually by techniques for a propelled affirmation). A sender scrambles data with the all-inclusive community key only the holder of the private key can disentangle this data.

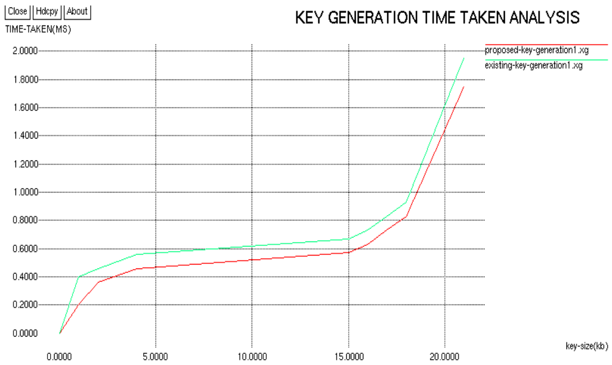


Fig. 3: Key Generation Time.

4.2. Packet delivery ratio

The estimation of Packet Delivery Ratio (PDR) depends on the got and produced bundles as recorded in the follow document. When all is said in done, PDR is characterized as the proportion between the got parcels by the goal and the created bundles by the source. Bundle Delivery Ratio is figured utilizing awk content which forms the follow record and creates the outcome.

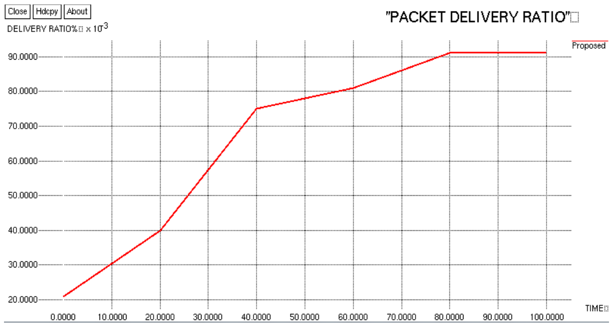


Fig. 4: Packet Delivery Ratio.

4.3. Bit error rate

While packets are transferring from one node to another node there are chances of getting errors in digital data. As shown in the figure the graph shows that even internal and external attacks occurred the bit error is reliable. We got effective graph results. The reliability of the communications channel is typically measured by the average bit error rate (BER). In computerized transmission, the quantity of bit blunders is the quantity of got bits of an information stream over a correspondence channel that have been changed because of commotion, impedance, bending or synchronization mistakes. The bit mistake rate (BER) is the quantity of bit blunders per unit time. The bit blunder proportion (likewise BER) is the quantity of bit mistakes separated by the aggregate number of exchanged bits amid a contemplated time interim. Bit blunder proportion is a unitless execution measure, frequently communicated as a rate.

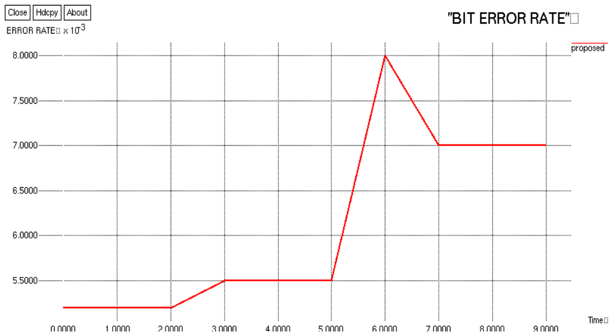


Fig. 5: Bit Error Rate.

4.4. Throughput ratio

The framework throughput or total throughput is the entirety of the information rates that are conveyed to all terminals in a system. Throughput is basically synonymous to advanced data transfer capacity utilization; it can be broke down numerically by applying the queueing hypothesis, where the heap in parcels per time unit is indicated as the landing rate (λ), and the throughput, where the drop in bundles per time unit, is signified as the flight rate (μ).

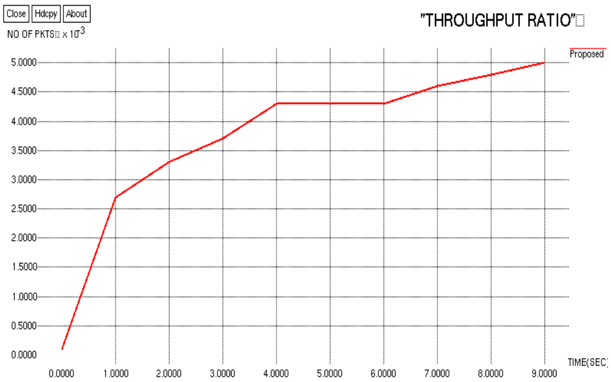


Fig. 6: Throughput Ratio.

We are implemented a four-way authentication protocol when two mix-zones are communication or when a person is moving from one mix-zone to another mix-zone area. This will improve the privacy of the mobile devices, when the mobile is travelling from two or more mix-zones. By implementing this authentication protocol, we can give privacy to user's.

5. Conclusion

In this paper our work will give an efficient four-way authentication protocol in mix zone model for privacy preservation to enhance the security. We had implemented a four-way handshake protocol while authenticating multiple mix-zones before data is exchanged between mix-zones. As compared to other protocol we had achieved better results. We also compare with the different authentication protocols like PAP, CHAP, and EAP. Our work will also compare with the previous existing methods based on several parameters and will give best performance.

References

[1] IEEE 802.11i: WLAN Security Standards, www.javvin.com/protocol80211i.html.

[2] Farshid Farhat, Somayeh Salimi, A. S. (2014). "Private identification, authentication and key agreement protocol with security mode setup." Iran Telecommunication Research Centre.

[3] Li, X. L. X. (2012). "Privacy preserving techniques for location based services in mobile networks." IEEE 26th International Parallel and Distributed Processing Symposium Workshops PhD Forum.

[4] G. Lowe, "Casper: A compiler for the analysis of security protocols," Journal of Computer Security, vol. 6, pp. 53–84, 1998.

[5] S. Xu, M. M. Matthews, and C.-T. Huang, "Modeling and Analysis of IEEE 802.16 PKM Protocols using CasperFDR," in IEEE ISWCS '08.

[6] http://www.lylebackemort.com/blog/2008/5/10/wpa-wpa2-asinsecure-as-i-expected,Accessed on 14 -03-2010.

[7] Sen Xu, Chin-Tser Huang, Manton M. Matthews, "Modeling and Analysis of IEEE 802.16 PKM Protocol using CasperFDR", University of South California, Columbia, SC 29208.

[8] Neetesh Saxena, N. S. C. (2013). "Extracting physical parameters of mechanical models from identified state-space representations." CSIT.

[9] SK Hafizul Islam, G. B. (2017). "A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication." Journal of King Saud

[10] University ¸S Computer and Information Sciences.

[11] Wei Xi, Chen Qian (2016). "Instant and robust authentication and key agreement among mobile devices." CCS