A STUDY ON WLAN SECURITY A LITERATURE REVIEW OF SECURITY IN WIRELESS NETWORK

P.Karunakar reddy[1], Dr.N.K.Shukla [2]

[1]Ph.D Research Scholar, Dept of CS, University of Allahabad,U.P, India.
[2]Professor, Dept of CS, University of Allahabad,U.P, India.

Abstract: -

As we know wireless networks have broadcast nature so there are different security issues in the wireless communication... The security traditions expected for the wired frameworks can't be extrapolated to remote frameworks. Programmers and interlopers can make use of the escape clauses of the remote correspondence. In this paper, we will think about the distinctive remote security threats to remote frameworks and traditions at exhibit open like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is more generous security tradition as contrasted and WPA in light of the fact that it uses the Advanced Encryption Standard (AES)encryption. There are few issues in WPA2 like it is powerless against savage power assault and MIC bits could be used by the software engineer to contrast it and the decoded content. So in this paper, we will focus on various sorts of remote security risks.

Keywords: Wi-Fi, Security, WPS

1. Introduction

Wireless communication is the exchange of data between two or more points that are not joined through an electrical connection, the most well known wireless technologies use electromagnetic wireless telecommunication, for example, radio. With radio waves separations could be short, for instance, two or three meters for the TV remote control or the degree that thousands or even immense number of kilometers for significant space radio correspondence. It incorporates diverse sorts of settled versatile and compact applications, including two-way radios, mobile phones singular PDAs and remote systems administration. Figure 1 demonstrates a case of remote correspondence. The different accessible remote 1 advancements contrast in nearby accessibility, scope range, and execution, and in a few conditions, the client must have the capacity to utilize various association composes switch between them utilizing related advances.

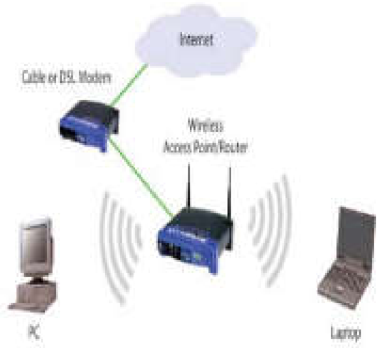


Figure 1 simple wireless communication

Wi-Fi is a remote neighborhood that empowers compact processing gadgets to interface effectively to the web. Institutionalized as IEEE 802.11 a/b/g/n, Wi-Fi approaches paces of a few sorts of wired Ethernet. Wi-Fi has turned out to be typical standard for access in private homes, inside workplaces, and open hotspots. Remote Wide Area Network (WWAN) - This system empowers you to get to the Internet by means of a remote wide region organize (WWAN) get to a card and a PDA or PC. These systems give a quick information speed contrasted and the information rates of versatile broadcast communications innovation and their range are likewise broad. Cell and portable systems in view of CDMA and GSM are great cases of WWAN. Remote Personal Area Network (WPAN) – These systems are fundamentally the same as WWAN with the exception of their range is exceptionally restricted. Remote Local Area Network (WLAN) - This system empowers you to get to the Internet in limited hotspots by means of a remote neighborhood (WLAN) get to a card and a PDA or workstation. It is a sort of neighborhood that utilizations high-recurrence radio waves instead of wires to impart between hubs. These systems give a quick information speed contrasted and the information rates of portable broadcast communications innovation and their range are exceptionally restricted. Wi-Fi is the most across the board and a famous case of WLAN innovation. Remote Metropolitan Area Network (WMAN) - This system empowers you to get to the Internet and sight and sound gushing administrations by means of a remote district zone arrange (WRAN). These systems give a quick information speed contrasted and the information rates of portable media transmission innovation and in addition different remote system.

Wireless LAN technology has rapidly become very popular all over the world. The wireless local area network (WLAN) protocol, IEEE 802.11, and associated technologies enable secure access to a network infrastructure Until the improvement of WLAN, the system customer should have been physically associated with the system by utilizing some sort of wiring.

With the quick increment in the utilization of WLAN innovation, it is critical to give a safe correspondence over the remote system. Since its creation, the security of remote systems experienced diverse phases of advancement, from MAC, deliver sifting or WEP to WPA/WPA2. The remote innovation was turned out to be extremely handy (not just) for home clients. Such a helpful alternative to be serenely associated with the web on a cell phone without the need of wires is as yet picking up in fame. This prompted an endeavor to make a setup of WLAN simpler for the normal client with no learning about software engineering. The aftereffect of this was standard known as Wifi Protected Setup (WPS).WPS, as an institutionalized innovation, is actualized on the wide assortment of at present created remote passageways. The wrong planning of its standard prompted deadly shortcoming which is talked about in this proposition in more noteworthy points of interest.

The 802.11 systems comprise of four noteworthy parts:

• DISTRIBUTION SYSTEM -a consistent part used to forward edges to their goal.

• ACCESS POINTS (APs)- gadgets playing out a remote to-wired crossing over capacity.

• Stations (STAs)- gadget with remote system interface speaking with other comparable gadgets through APs.

• WIRELESS MEDIUM-the medium used to exchange outlines from station to station.

Weakest Security Mechanisms

Among the most commonly used security mechanisms toprotect WLAN while them being no obstruction at all for an even unexperienced attacker are SSID hiding and

MAC ADRESS FILTERING:

Many APs offer the client an alternative to concealing the SSID. In the event that it is empowered, the AP in its guide outlines does not demonstrate the SSID - an unfilled string has appeared. In spite of the fact that it would seem that a smart thought (if nobody sees the WLAN it can't be assaulted), it isn't useful in any way.

MAC ADRESS FILTERING:

Like SSID concealing, MAC address sifting is likewise normally utilized "security" instrument. Despite the fact that it is smarter to utilize even frail insurance than none by any stretch of the imagination, MAC address sifting can be effectively broken by utilizing MAC address satirizing procedure.

WEP (Wired Equivalent Privacy) :

Wired Equivalent Privacy (WEP) is a security calculation for IEEE 802.11 remote systems.

WEP Encryption

For every bundle, a 24-bit instatement vector (IV) is picked. The IV linked with the root key yields the per parcel key. The CRC-32 is computed over the information to be encoded. The per parcel key is then utilized to encrypt the information taken after by the ICV utilizing RC4 stream figure. The (decoded) IV is transmitted in the header of the bundle.

2. Background Study

This part is worry of the remote security utilizing Wi-Fi Protected Access 2(WPA2).Before talking about Wi-Fi ensured get to 2, examine foundation contemplate has been Related to remote Security.

2.1Need of Wireless Security

Security is one of essential test which is to be taken care of in the period of remote innovation nowadays. Current security principles have demonstrated that security isn't staying aware of the developing utilization of remote innovation. Each time new powerlessness comes in presence to the current remote benchmarks. Remote security is the counteractive action of unapproved access or harm to PCs utilizing remote systems. Remote systems are extremely normal, both for associations and people. Numerous PCs pre-introduced remote cards. Be that as it may, the remote systems administration has numerous security issues yet the capacity to enter into a system utilizing remote innovation has incredible advantages over the wired association. Programmers have discovered remote systems generally simple to break into, and even utilize remote innovation to split into wired systems. Accordingly, it's essential that undertakings characterize successful remote security strategies that make preparations for unapproved access to vital assets. Remote Intrusion Prevention Systems are usually used to uphold remote security strategies. The dangers to clients of remote innovation have expanded as the administration has turned out to be more well known. Be that as it may, there are numerous securities related to the present remote convention and encryption strategies in the inconsiderateness and obliviousness that exist at the client and corporate IT level. Breaking technique has turned out to be significantly more advanced and inventive with the remote. Breaking has likewise turned out to be substantially less demanding and more open with simple to utilize windows or Linux-construct devices being made accessible in light of the web at no charge.

2.2 Security threats to wireless networks

Security of remote systems implies assurance from assaults on secrecy, uprightness, and accessibility. Conceivable dangers originate from vulnerabilities in the security conventions. This area clarifies different sorts of security assault procedures. These procedures can be connected to disregard both classification and uprightness or just secrecy and just respectability [1]. Movement Analysis: This strategy empowers the assailant to have the entrance to three kinds of data. The main kind of data is identified with the recognizable proof of exercises on the system. The second kind of data for the assailant is critical to get the distinguishing proof and physical areas of a passage in its environment. This third kind of data for an aggressor can be acquired by activity examination of the data about the correspondence convention. An assailant needs to assemble the data about the size and the quantity of the bundle over a specific timeframe. Spying: if there should arise an occurrence of spying assailant covertly tunes in to the private discussion of others without their consent. Listening stealthily assaults incorporate aloof spying, dynamic spying with halfway known plaintext and dynamic spying with known plaintext. Aloof listening stealthily is accustomed to viewing over a boundless remote session. Latent spying with halfway known plaintext compose assault, the aggressor watches over a remote session an effectively infuses claim message so as to uncover the substance of the messages in the session.

Man in center assault empowers information perusing from the session. There are a few different ways to execute this sort of assaults. One way is when aggressor upsets the session and does not take into account the station to set up correspondence again with the Access Point; AP station endeavors to build up the session with the remote system through AP, however, can do that exclusive through the workstation of the assailant putting on a show to the AP. In the meantime assailant sets up association a confirmation with the AP, now there are two scrambled passages rather than one is set up amongst assailant and AP, while the second one is set up amongst aggressor and the station. This empowers assailant to have the entrance to the information traded between the working station and rest of the system. ARP assault is a subtype of man in the center assault since these assaults are coordinated towards one segment of the remote customers. The assailant escapes verification or give false accreditations by this sort of assault. In high-jacking kind of assault, the aggressor denies the genuine proprietor of the approved and verified session .the proprietor realizes that he has no entrance to the session any more however doesn't know that the assailant has assumed control over his session and trust that he lost the session because of customary needs in organize working once the assailant assume control over a legitimate session he can utilize it for different purposes over a specific timeframe. These assaults occur progressively. Replay assault is use to get to the system through approval. The session that is under an assault does not change or upsets at all. This does not occur continuously. The aggressors get the entrance to organize after the first session terminates. Foreswearing of Service (DoS): an assailant messes with the information before it is conveyed to the sensor hub. It causes a disavowal of administration assault because of wrong or deluding data. Sticking is One of DoS assault on arrange accessibility. It is a performed by malignant assailants who utilize different remote gadgets to impair the correspondence of the clients in authentic remote system. Word reference building assaults: In these sorts of assaults an assailant experiences a rundown of hopeful passwords one by one; the rundown might be unequivocally specified or numerated or verifiably characterized, can fuse information about the casualty, and can be semantically inferred. Word reference building assaults are conceivable in the wake of examining enough movement on a bustling system. To maintain a strategic distance from these dangers and enhance the security of the remote systems different organizations worked together to make the Wi-Fi Alliance to make the powerful security convention. At first, they accompany the new security convention for remote system different organizations worked together to make the Wi-Fi Alliance to make the hearty security convention for the remote system known as Wi-Fi Protected Access (WPA). The WPA convention executes most of the IEEE 802.11i standard, and was expected as a middle of the road the measure to replace WEP. WPA utilizes the transient key joining measure to replace WEP. WEP utilizes the Temporal Key Integration Protocol (TKIP) calculation for encryption. TKIP is security convention utilized in the IEE E 802.11i remote systems administration standard. TKIP is composed by IEEE802.11i undertaking gathering and the Wi-Fi Alliance as the answer for supplant WEP without requiring the substitution of inheritance equipment. This was important on the grounds that the support the WEP had left Wi-Fi systems without feasible connection layer security, and an answer was required for as of now sent hardware[2].

WPA has following advantages:

• A cryptographic Message Integrity Code (MIC), called Michal, to crush frauds. Message Integrity Code (MIC) is processed to identify blunders in the information substance, either because of exchange mistakes or because of intentional shifts. This avoids man in the center assault, disavowal of administration assault.

• another Initialization Vector (IV) sequencing discipline, to expel Replay assaults from the attacker`s stockpile.

• A rekeying instrument, to give crisp encryption and respectability keys, fixing the danger of assaults originating from key reuse. In this manner gives security against listening stealthily assaults.

In spite of the fact that the WPA convention has expanded remote security, all things considered, it additionally has a few issues.

• Weakness in passphrase decision in WPA Interface: This shortcoming on in view of Pairwise Master Key (PMK) that is gotten from the connection of the passphrase, Service Set Identifier (SSID), length of the SSID and nonces.

• The likelihood of the Brute Force Attack: Brute power is thought to be a latent assault in which the interloper will produce each conceivable change in the key and attempt to unscramble the scrambled message with each created stage, and approve the yield of methods for cross-correlations with words, File header some other information.

• Placement of MIC: It is viewed as an issue since it very well may be us by any programmer nullifying the substance of the decoded message joined with the savage power assault.

After the WPA new convention came which is called Wi-Fi Protected Access 2 (WPA2) The IEEE 802.11i standard otherwise called Wi-Fi Protected Access 2 (WPA2) is an alteration to the 802.11 standard indicating security components for remote systems. The draft standard was approved on June 24th, 2004, and replaces the past security determinations, Wired Equivalent Privacy (WEP), which was appeared to have serious security shortcomings. Wi-Fi Protected Access (WPA) had already been acquainted as a halfway arrangement with WEP weaknesses. WPA actualized just a subset of IEEE 802.11i. WPA2 makes utilization of a particular method of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message

Validation Code (CBC-MAC) convention (CCMP). CCMP gives the two information privacy (encryption) and information uprightness. The utilization of the Advanced Encryption Standard (AES) is a more secure other option to the RC4 stream figure utilized by WEP and WPA. 3. Wi-Fi Protected Accesses 2 The WPA2 standard has two segments, encryption, and verification which are significant to a safe remote LAN. The encryption bit of WPA2 orders the utilization of AES (Advanced Encryption Standard) yet TKIP (Temporal Key Integrity Protocol) is accessible for in reverse similarity with existing WAP equipment. The validation bit of WPA2 has two modes: Personal and Enterprise. The Personal mode requires the utilization of a PSK (Pre-Shared Key) and does not expect clients to be independently validated. The Enterprise mode, which requires the clients to be independently validated in light of the IEEE 802.1X confirmation standard, utilizes the Extended EAP (Extensible Authentication Protocol) which offers five EAP norms to look over: EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), Protected EAP vo/EAP-Microsoft's Challenge Handshake Authentication Protocol v2 (PEAPvo/EAPMSCHAPv2), Protected EAP v1/EAP-Generic Token Card (PEAPv1/EAP-GTC) and EAP-Subscriber Identity Module of the Global System of Mobile Communications (EAP-SIM). The Enterprise mode has the accompanying equipment/programming usage prerequisites:

- Selection of EAP composes that will be bolstered on stations, APs (Access Point), and confirmation servers.

- Selection and sending of verification servers regularly RADIUS (Remote Authentication Dial-in User Service) based validation servers.

- WPA2 programming overhauls for APs and customers.

WPA2 builds up a safe correspondence setting in four stages. In the principal stage the gatherings, AP, and the customer will concede to the security arrangement (validation technique, the convention for unicast activity, the convention for multicast movement and pre-verification strategy) to utilize that is upheld by the AP and the customer. In the second stage (relevant to Enterprise mode just) 802.1X verification is started between the AP and the customer utilizing the favored confirmation strategy to create an MK (normal Master Key). In the third stage after an effective verification, brief keys (each key has the restricted lifetime) are made and consistently refreshed; the general objective of this stage is key age and trade. In the fourth stage, all the beforehand created keys are utilized by the CCMP convention to give information privacy and uprightness.

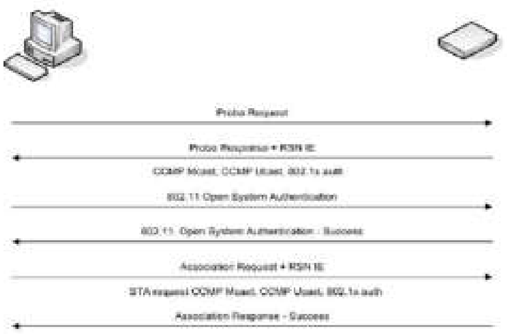

Probe Request
Probe Response + RSN IE
CCMP Mcast, CCMP Ucast, 802.1x auth
802.11 Open System Authentication
802.11 Open System Authentication : Success
Association Request + RSN IE
STA request CCMP Mcast, CCMP Ucast, 802.1x auth
Association Response - Success

Figure 2. Agreeing on the security policy

3.1 WPA2 Authentication One of the real changes presented with the WPA2 standard is the partition of client verification from the implementation of message respectability and protection, in this manner giving a more versatile and strong security engineering appropriate to home systems or corporate systems with break even with ability. Validation in the WPA2 Personal mode, which does not require a confirmation server, is performed between the customer and the AP creating a 256-piece PSK from a plain-content passphrase (from 8 to 63 characters). The PSK in conjunction with the Service Set Identifier and SSID length frame the scientific reason for the PMK (Pair-wise Master Key) to be utilized later in key age. Validation in the WPA2 Enterprise mode depends on the IEEE 802.1X verification standard. The real segments are the supplicant (customer) joining the system, the authenticator (the AP fills in as the authenticator) giving access control and the confirmation server (RADIUS) settling on approval choices. The authenticator (AP) isolates each virtual port into two sensible ports, one for benefit and the other for validation, making up the PAE (Port Access Entity). The confirmation PAE is constantly open to permit verification outlines through, while the administration PAE is just open upon fruitful validation by the RADIUS server. The supplicant and the authenticator convey utilizing Layer 2 EAPoL (EAP over LAN). The authenticator changes over EAPoL messages to RADIUS messages and after that advances them to the RADIUS server. The validation server (RADIUS), which must be good with the supplicant's EAP composes, gets and forms the confirmation ask. Once the validation procedure is finished the supplicant and authenticator have a mystery MK (Master Key) has appeared in Figure 3.

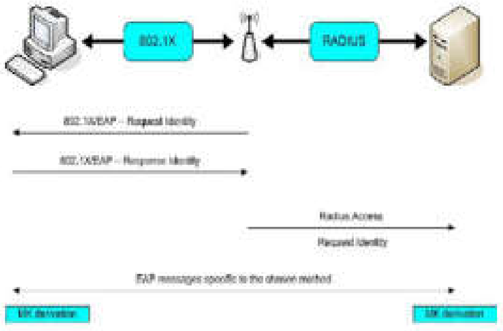

802.1X
RADIUS
802.1X/EAP – Request Identity
802.1X/EAP – Response Identity
Radius Access
Request Identity
EAP messages specific to the chosen method
MK derivation
MK derivation

Figure 3. 802.1X authentication

3.2 WPA2 Key generation

WPA2 key age is proficient by methods for two handshakes: a 4-Way Handshake for PTK (Pairwise Transient Key) and GTK (Group Transient Key) deduction, and a Group Key Handshake for GTK recharging. The 4-Way Handshake, achieved by four EAPoL-Key messages between the customer and the AP, is started by the passage and plays out the accompanying errands:

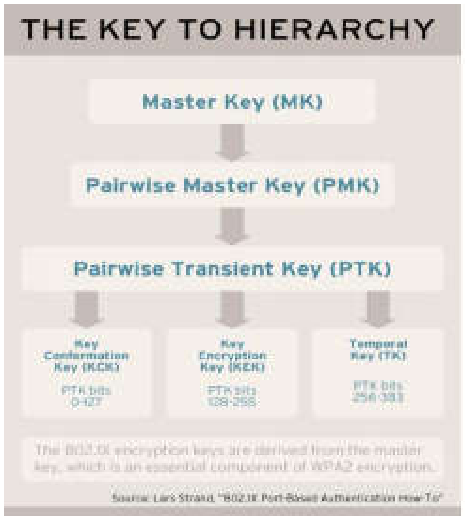
- Confirm the customer's information of the PMK. The PMK inference, required to create the PTK, is reliant on the verification

- Method utilized. In WPA2 Personal mode the PMK is gotten from the verification PSK and for WPA2 Enterprise mode, the PMK is gotten from the confirmation MK (enter chain of importance in Figure 3).

- Derive a crisp PTK, which is contained three sorts of keys: KCK (Key Confirmation Key – 128 bits) used to check the honesty of EAPoL-Key casings, KEK (Key Encryption Key – 128 bits) used to scramble the GTK and the TK (Temporal Keys – 128 bits) used to anchor information movement.

- Install encryption and respectability keys.

• Encrypt transport of the GTK which is computed by the AP from an arbitrary GMK (Group Master Key). • Confirm the figure suite determination



The 802.1X encryption keys are derived from the master key, which is an essential component of WPA2 encryption.

Source: Lars Strand, "802.1X Port-Based Authentication How-To"

The Group Key Handshake is only used to disassociate a host or renew the GTK and uses the KEK generated during the 4-Way Handshake to encrypt the GTK.

3.3 WPA2 Encryption

The AES utilized by WPA2 "is a square figure, a sort of symmetric key figure that utilizations gatherings of bits of a settled length – called squares" [13]. A symmetric key figure is an arrangement of guidelines or calculation that uses a similar key for both encryption and unscrambling. In the WPA2/802.11.i usage of AES, bits are scrambled (utilizing a 128 piece key length) in squares of plaintext, that are ascertained autonomously, instead of a key stream acting over a plaintext information input stream. AES encryption incorporates 4 arranges that make up one round and each round is iterated 10 times. AES utilizes the Counter-Mode/CBC-Mac Protocol (CCMP). CCM is another method of task for a square figure that empowers a solitary key to be utilized for both encryption and confirmation (with various introduction vectors). The two hidden modes utilized in CCM incorporate Counter mode (CTR) , that accomplishes information encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to give information trustworthiness. CBC-MAC is utilized to produce a confirmation segment because of the encryption procedure (Figure 5). This is not quite the same as earlier Message Integrity Code (MIC) usage, in which a different calculation for honesty check is required. To additionally improve its propelled encryption capacities, AES utilizes a 128-bit Initialization Vector (IV).

3.4 WPA2 Encryption Steps

The MIC - like a checksum - gives information honesty to the non alterable fields in the 802.11 header, not at all like WEP and WPA, keeping parcel replay from being misused to decode the bundle or trade off cryptographic data. The MIC is ascertained utilizing a 128-piece IV as takes after:

- IV is scrambled with AES and TK to create a 128-piece result.

- 128-bit result is XOR with the following 128 bits of information.

- The aftereffect of XOR is then gone through stages 1 and 2 until the point when every one of the 128 squares in the 802.11 payloads is depleted.

- At the finish of the task, the initial 64 bits are utilized to deliver the MIC.

- The Counter Mode calculation encodes the information and the MIC (ascertained by utilizing the CBC-MAC). The Counter Mode calculation starts with a 128-piece counter preload like the MIC IV, however, utilizes a counter esteem introduced to 1 rather than an information length bringing about an alternate counter used to scramble every bundle. The information and the MIC are encoded as takes after:

- Initialize counter on the off chance that it is the first run through generally increase counter.

- First 128 bits are encoded utilizing AES and TK to create a 128-piece result.

- An XOR is performed on the aftereffect of stage 1. The initial 128 bits of information creates the initial 128-piece encoded square.

- Repeat stages 1-4 until the point when all the 128-piece squares have been encoded.

- Set counter to zero and encode it utilizing AES and XOR with MIC adding the outcome the scrambled casing.

3.5 Benefits of WPA2

WPA2 (alongside WPA) settled vulnerabilities of WEP to "programmer assaults, for example, 'man-in-the-middle', confirmation producing, replay, key impact, powerless keys, bundle fashioning, and 'brute– constrain/lexicon' attacks"[13]. By utilizing government review AES encryption and 802.1X/EAP verification WPA2 additionally upgrades the changes of WPA utilizing TKIP encryption and 802.1X/EAP confirmation over WEP's blemished encryption key execution and its absence of validation. "AES has no known assaults and the present examination shows that it enjoys 2120 activities to reprieve an AES key"[13]. Notwithstanding the encryption benefits, WPA2 additionally adds two upgrades to help quick wandering of remote customers moving between remote AP's. PMK storing support – takes into account reconnections to AP's that the customer has as of late been associated without the need to re-confirm.

Pre-confirmation bolster – enables a customer to authenticate with an AP towards which it is moving while as yet keeping up an association with the AP it's moving far from. PMK reserving backing and Pre-confirmation bolster empower WPA2 to decrease the meandering time from over one moment to under 1/tenth of a second. A definitive advantage of the quick meandering is that WPA2 would now be able to help timing-touchy applications like Citrix, video, or VOIP (Voice over IP) which would break without it.

4. Literature Review

The Kirti Raj Bhatele,[3] exhibited half breed security convention for better security utilizing a mix of both symmetric and Asymmetric cryptographic Algorithms. In this hash estimation of the unscrambled message utilizing AES calculation is computed utilizing MD5 calculation. This hash esteem has been encoded with double RSA and the scrambled message of this hash esteem likewise sent to goal. Presently at the less than desirable end, hash estimation of unscrambled plaintext is ascertained with MD5 and afterward it is contrasted and the hash estimation of unique plaintext which is figured at the sending end of its honesty. By this we can know whether the first content being modified or not amid transmission in the correspondence medium.

ArashHabibiLashkari,[4] introduced a study on remote security conventions (WEP, WPA, and WPA2/802.11i). Here WEP conventions compose, shortcomings and upgrades, WPA conventions compose, WPA changes, for example, cryptographic message respectability code or MIC, new IV sequencing discipline, per bundle key blending capacity and rekeying instrument. They additionally clarified the significant issue on WPA that occurred on PSK part of the calculation. At last paper clarified third era of remote security convention as WPA2/802.11i.

GamalSelim,[5] clarified different kinds of security assaults adjustment, manufacture, capture, savage power, practicality, and static position of a MIC. They studied as of now accessible security conventions that are WEP, WEP2, and WPA2. They additionally proposed another component called numerous space framework (MSS). MSS influence utilization of the key selector, to space selector and MIC, rearrange selector, MSS utilizes one of four encryption calculation RC4, RSA, Blowfish, and AES.

LifenSang,[7] Shared mystery free security foundation for remote systems in view of two physical natives. Helpful sticking and spatial flag requirement Cooperative sticking is for classified remote correspondence and spatial flag implementation is for message credibility. The proposed foundation gives privacy, character, validation, message verification, respectability, non-denial, collector non-revocation secrecy.

Andrew Gin,[8]Compared the execution examination of developing the remote 802.11security design. Paper clarified remote system security strategies. Paper clarify security layers like WEP shared key validation and 40 bit in encryption WEP shared key confirmation and 104 piece encryption, WPA with PSK verification and RC4 encryption, WPA with EAP – TLS confirmation RC4 encryption, WPA2 with PSK validation and AES encryption and WPA2 with EAP – TLS verification and AES encryption. Consequences for Throughput are additionally neglected.

Floriano De Rango,[9] Proposed static and dynamic 4-way handshake solutions to avoid denial servicer attack in WPA and IEE 802.11i. Paper also explained DoS and DoS flooding attack against IEE802.11i 4-way handshake.

6. References

[1] S.D.Kanawat and P.s.Parihar,Editors, “Attacks in Wireless Networks”, International jornal of Saart Sensors amdAdhoc Networks,(2011) May 18-23

[2] Y.X.Lim and T.SChmoyer, “Editors,Wireless Intrusion Detection and response”, IEEE Information Assurance Workshop,(2003) June18-20,westpoint,New York

[3]A.Sinhal and M.Pathak,Editors, “A Novel Approach to the Design of New Hybrid Security rotocol Architecture”, IEEE international Conference on Advanced Communication Control and Computing Technologies(ICACCCT),(2012) August 23 Ramanadhapuram.

[4] A.H.Lashkari and M.M.S. Danesh, Editors, "A Survey on Wireless Security Protocols, WEP, WPA and WPA2/802.11i",IEEE international Conference on Computer Science and Information Technology,(2009) august 8-11 Beijing.

[5]G.Selim, H.M.E. Badawy and M.A. Salam, Editors, "New Protocol Design For Wireless Network Security", IEEE international Conference on Computer Science and Information Technology, (ICACT), (2006) feb 20-22 .

[6] H.W.Lee, A.S.K. Pathan and C.S. Hong Editors, "Security in Wireless Sensor Networks, Issues and Challenges", international Conference on Advanced Communication Technology (ICACT) (2006) feb 20- 22 phoenix park.

[7] L.SangandA.Arora Editors, "A Shared Secret Free Security Infrastructure For Wireless Network", ACM Transactions on Autonomous and Adaptive System (TAAS) (2012) July

[8] A.Gin and R. Hunt, Editors, "Performance Analysis Of Evolving Wireless IEEE 802.11 security Architectures", ACM international Conference on Mobile Technology Application and Systems (2008) [9] F.DeRango ,D.C.LentiansS.Marano, Editors, "Static and Dynamic Four way handshake Solution to avoid Denial of Service Attack in Wi-Fi Protected access and IEEE 802.11i",EURASIP, Journal on wireless Communication and Networking (2006) June

[10]"IEEE 802.11i." Wikipedia, The Free Encyclopedia. 11 Nov 2006, 10:22 UTC. Wikimedia Foundation, Inc. Nov. 25 2006

[11]"Wi-Fi Protected Access 2 Data Encryption and Integrity." Microsoft TechNet. The Cable Guy. July 29 2005.

[12]"Understanding the updated WPA and WPA2 standards". ZDNet Blogs.PostedbyGeorgeOu. June 2 2005.

[13]"Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise." Wi-Fi Alliance, Feb. 27 2005

[14]Lehembre, Guillaume. "Wi-Fi security –WEP, WPA and WPA2". Article published in number 1/2006 (14) of hakin9, Jan. 2006. Publication on www.hsc.fr on Dec. 28 2005.

[14]Ou, George. "Wireless LAN security guide".www.lanarchitect.net. Revision 2.0 Jan 3 2005 [15]Bulk, Frank. "Learn the basics of WPA2 WiFi security". Network Computing Jan. 27 2006. "Extensible Authentication

Protocol." Wikipedia, The Free Encyclopedia. Nov. 26 2006, 15:39 UTC. Wikimedia Foundation, Inc. Nov 27 2006

[16]Gupta, Ashok and Buthmann, Theresa. “The Bell Labs Security Framework: Making the case for End-to-End Wi-Fi Security”. Lucent Technologies Sep. 11 2006 (15).