Overview of 802.16 Security: A Survey Paper

Voora Lakshmi Haneeja[1], Shaik Jasmin[2]

[1]Student Dept. of SCSE, Lovely Professional Univerity, Phagwara, Punjab, India
[2]student, Dept. of SCSE, Lovely Professional University, Phagwara, Punjab, India

---***---

Abstract: This study examines some unresolved essential security problems in the IEEE 802.16 a standard family. The allocation of powerful resources, and the mesh mode, two of the standard's most critical features, has also been shown to be vulnerable to an attack that poses serious challenges to a communication protection and confidentiality. In the first instance, the invader insist minimize the bandwidth available to his neighbors in an attempt to acquire extended assets as long as invader needed; in the second instance, we percept there might be no accurate privacy in convey among a network areas of mesh. In contempt of most recent adaptation, 802.16e of IEEE, which patches formerly asserted security breaches, this danger still exists.

Keywords: Architecture, Security, Algorithms, Privacy, Key Exchange, Authentication, Authorization.

Introduction:

IEEE 802.16[1] security definitive form is wireless metropolitan area networks (WMANs), primarily refined to inscription "a last mile" issue. Previously, predominant broadband industries and clients inappropriately believe that, the most common security flaws utilize 56-bit of Data Encryption Standard (DES) algorithm. In reality, size of the key is most commonly irrelevant safety vulnerabilities.

802.16 of IEEE is a wireless broadband communication protocol that can be used as a last-mile alternative for cable and DSL. Without the need for a router, 802.16 standard would arrange secure, strolling ,compact , and in the end of mobile wireless networking.

By installing standards already in IEEE 802.16, IEEE 802.16 Working Groups aims to avoids bug fixes [2-5] in IEEE 802.11. The Data Over Cable Service Interface Specifications standard had created to address end most cable issues. Since both IEE 802.16 and cable are broadband technologies, they keep incompatible threat models. As a result, 802.16 protection failed to secure 802.16 links of IEEE.

This paper provides an outline of IEEE 802.16 securities as well as a review of the crucial security vulnerabilities. As well also we recommend changes on to defend the standard contrary to assault. Most of 802.16 ellipsis used in this paper are specified in a report.

IEEE 802.16 Architecture:

The IEEE standard 802.16 is made up of a protocol stack with clearly stated interfaces. Three sublayers help compensate the physical layer and MAC layer. Mac Layer compromises of the MAC Common Part Sublayer (MACCPS), and the Service Specific MAC Convergence Sublayer (MACCS).

Among MAC CPS and Physical Layer is the Privacy Sublayer. It's the sublayer supervise of encrypting and decrypting data when it enters and exits the PHY layer (Physical Layer), as well as secure key exchange and attestation. It also encourages DES 56-bit traffic encryption and triple-DES key exchange encryption. Different cryptographic suites and encryption protocols, such as AES, can be used because of the standard's modular design.

The MAC CPS is the backbone regarding this level. Through this case sublayer orders as long as Interconnection control, bandwidth allotment along with methodology network entry is all described. And it works as an uplink setting, bandwidth appeal and provide, ARQ (automatic duplication request) and connection control also defined. On this Media access control layer the Interconnection within Convergence sublayer and MAC Common Part Sublayer, they execute at this MAC SAP (MAC service Access Point). Transmission is as easy as at most one primary action.

The four principle methods of IEEE 802.16 are physical layer provides notable pliability. This is flexibly authorize to work on a extensive variety on range distribution, together with channel bandwidth variation, duplex frequency separation, and duplex time separation. Although, all methods assists a standard attributes set, along with primary start up process, bandwidth appeal, and channels aimed at conductance and end user communication facts. The 802.16 security protocols of IEEE are remains same, except for the Physical Layer type. IEEE 802.16 splits air connections to frames. Downlink frames (from BS (base station) to the SS (Subscriber station)) retrains a frame header, which comprehend 2 slot maps, 1DL_MAP(Downlink)and1UL_MAP(Uplink). These maps are showing location, size, and coding of all posts through downlinks as well as private uplinks.

Media access control layer is directed to the Interconnection. Each and every building is yours on a specific connection, identified by the connecting ID. Management connection handles streaming data, for the first time ranging from, bandwidth seeks, along with general management texting. For every Subscriber Station, the second administrative attachment conveys the Internet Protocol administration packages. Utterly other communications are travel communications. The 802.16 of IEEE link management function is dynamic generates transport connections to manage end user packets.

IEEE 802.16 only secure transport communications along with secondary management stations.

MAC Protocol Data Unit packet format:

IEEE 802.16 generates packets or MAC data tracking sections - to move facts over communication. MPDUs divided in two parts, evolve by the MPDU head, as Figure 1 shows:

- BRH (Bandwidth request header), where the header is entity pack; and
- GMH (generic MAC header), subsequently by payload and optional CRC (cyclic redundancy checking).

Connection ID recognise management packets. Each MPDU administration coveys individual MAC management message. Transportation connections conveys to lead service data units by MAC - data units send by network stacks over MAC. IEEE 802.16 MAC protocol offers more variability in how MPDUs treat MSDUs.

Network installation:

Network installation includes series of actions:

1. Subscriber Station checks the appropriate Base station downlink signal, i.e. utilize to initiate channel framework.

2. Commencing configuration permits a Subscriber Station to set Physical layer variables appropriately and primary management channel via BS. These channel is pre-owned for skills intervention, authority, and critical management.

3. PKM protocol approves Subscriber Station in Base Station.

4. Subscriber Station enrol by dispatch a message request to Base Station. Base Station response provides connection IDs for subordinate management connection.

5. Subscriber Station and Base Station build send links using MAC_create_connection application. Application to genrates a powerful dynamic transport Interconnection exhibits if MAC encryption is required.

Security Algorithms of 802.16:

In 802.16e security of IEEE is enforce a secret sublayer under Media Access Control protocol. Its target is to impart access control as well data connection privacy.

These security construction of 802.16 of IEEE utilize 5 phases, which are defined in the succeeding sections.

X.509, Privacy Key Management authorization protocol,

Security Associations, Privacy and Key Management (PKM) and Encryption.

Security Associations:

SAs supports the reliability status of each and every network connection. 802.16 usage of two Security associations phases yet only SA facts are effectively described. Data Security associations securely conveys within Subscriber Station and Base Station.

Data SA has the subsequent features

- 16bit SA identifier (SAID)
- Secure data protection cipher. Normal use Data Encryption Standard in CBC (cipher block chaining) mode [7], yet this pattern is extended for further algorithms.
- Two TEKs (traffic encryption keys) to encryption of data: current operation key and Traffic Encryption Key for when the current key terminates.
- Two 2-bit key identifiers, one per TEK.
- TEK life time. The default value for this parameter is also half a day it takes a minimum of 30 minutes and a maximum of seven minutes days.
- A 64-bit setup tracks for each and every TEK.
- SA data type index. Initial SAs were established during the link loading. static SAs composed in Base Station; whereas dynamic SAs built as vital for capable transport connections.

To defend transport connectivity, Subscriber Station prepares a SA data to use create_connection to request. To reinforce multicast, requirement permits multiple connection IDs to claim SA. At the mesh entry, IEEE 802.16 security creates Security Association perpetually for the second administration channel. A secure (SS) Subscriber Station hence it has 2 or 3 SAs, single for the second administration channel and other one for the uplink and downlink transport links or divide SAs for uplink and downlink. Each multicast network party also is need SA to participate within batch members.

The authority of Security Association, which is an unspecified quality, contains

- X.509 certificate recognise Subscriber Station (SS).
- 160-bit authorization key. The accurate to make use of this key specifies authorization to utilize 802.16 of IEEE transport links.
- 4-bit load recognition for Authorization Key (AK).
- AK endurance, fluctuate from 1 day to 70 days. The lapse time is 7 days.
- Encryption key (3-DES of 112 bit) in order to dispense TEKs. Key Encryption key (KEK) is arranged as:

KEK = Truncate-128 (SHA1 $(((AK \mid 0^{64}) \oplus 53^{64}))$,

where Truncate-128 (·) means get rid of each and everything excluding the original 128 pieces of parameter,

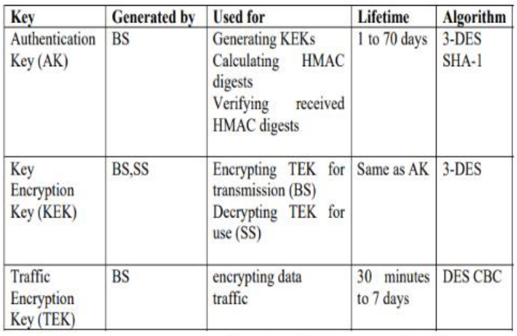
a | b means a mixture of strings a and b,

$\oplus$ mean Exclusive-OR,

a^{n} means octet a iterate n times, and SHA1 is defined by a safe hash level.

- Downlink HMAC key that dispense data authentication for key distribution communication from Base Station to Subscriber Station. This key is organized as: Downlink HMAC key =SHA1 $((AK \mid 0^{44}) \oplus 3A^{64})$.
- HMAC uplink key allows data authentication for crucially divide messages via SS to BS. The HMAC uplink key is organized as: Uplink HMAC key = SHA1 $((AK \mid 0^{44}) \oplus 5C^{64})$.
- files of SA data authorized.

SA authority is split by the state within a specific BS and specific SS. The pattern takes these 2 channels to keep AK as a confidential. BS utilizes SA authority to amend SA to SS.



Key	Generated by	Used for	Lifetime	Algorithm
Authentication Key (AK)	BS	Generating KEKs Calculating HMAC digests Verifying received HMAC digests	1 to 70 days	3-DES SHA-1
Key Encryption Key (KEK)	BS,SS	Encrypting TEK for transmission (BS) Decrypting TEK for use (SS)	Same as AK	3-DES
Traffic Encryption Key (TEK)	BS	encrypting data traffic	30 minutes to 7 days	DES CBC

Table 2: Summary of the cryptographic keys used with SAs [5]

X.509 certificate profile:

It recognise communication among groups. The standard describes X.509 Certificate profile needs the succeeding fields:

- X.509 certificate configuration version three[8].
- Certificate sequential number.
- Certificate provider's signature algorithm public key Cryptography Standard 1 i.e., RSA encryption and also SHA1 hashing.
- Certificate provider.
- Certificate validity time.
- Certificate title — i.e, certificate holder recognition, which, whether the title is the SS, involve the MAC address of the channel.
- The title of the title community, which gives the certificate the owner's public key, indicates what the public key looks like has been utilized, and it is forbidden from RSA attacks.
- Signature algorithm, that is exactly similar to certificate provider's algorithm.
- Provider's Signature, that is a also digital signature of the Abstract Syntax Notation distinguish encoding rules encryption for the rest of remaining certificates.

802.16 of IEEE did not specify extensions of X.509 certificates.

The definitive determines to two categorize of certificates: manufacturer certificates and Subscriber Station certificates. It did not enumerate Base Station certificates. The manufacturer's certificate recognize the manufacturer of the 802.16 of IEEE system. These could be an independent certificate or provided by a third party end user. Subscriber Station certificate discovers the specific SS as well as assess its MAC address to the subject field.

Manufacturer's usually generate and inscribe Subscriber Station (SS) certificates. The Base Station (BS) generally utilize the manufacturer's certificate public or social key Verification of Subscriber Station certificate, therefore verified the device as authentic. This pattern supposed such that the SS retain it confidential key identical to its own public key in a bit way closed memory, which prevents attacker from being efficiently destroyed.

Privacy and Key Management authorization:

These protocol divides authority key to certified Subscriber Station. The authorization protocol contains of 3-message exchanges within Subscriber Station SS and a base station BS. The SS commence the law by dispatching the starting two messages, at the same time BS replies includes a third message.

Message-1:

SST → BST Cert (Manufacturer (SST))

Message-2:

SST → BST Cert (SST) | Capability |SAID

Message 3:

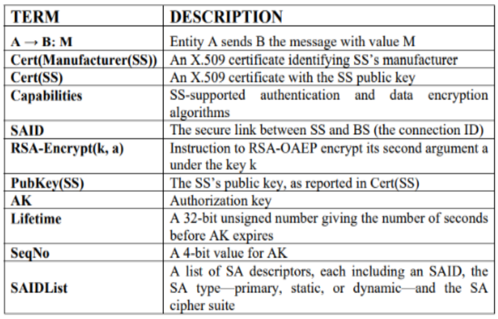
BST → SST RSA-Encrypt (PublKey (SST), AKey) | All Life | SeqNum | SAIDLists

SST (subscriber station) utilize Message-1 to press its X.509 certificate Cert (Manufacturer (SST)) to BST (Base station), which utilize it to determine even if the SST (subscriber station) is a reliable system. These pattern thinks that all networks from a reputable manufacturer can be worthy of trust. 802.16e permits Base Station to disregard this message as its security strategy might only permits entry to priori-familiar devices.

Subscriber Station transmits Message-2 shortly succeeds Message-1. Message-2 contains X.509 Cert

(SST) SST certificate, of which security skills, and Identifies SAID of what you will have to do its own main SST (Subscriber station). Cert (SS) allows Base Station (BST) to decides if SS permits the public key for the Cert (SST) allows BST(Base station) to create Message-3.

If Base Station could demonstrate Cert (SST) and Subscriber Station are approved, it Acknowledge with Message-3, who confirms SA authorized within 2-channels. Actual usage of this Authorization Key indicates authority to entry the Wireless MAN channel. The pattern suppose that particular Base Station and Subscriber Station retain the Authorization Key – i.e., the pattern key is not admit to the any of other party. 802.16 of IEEE does not restrict the production of this key.



TERM	DESCRIPTION
A → B: M	Entity A sends B the message with value M
Cert(Manufacturer(SS))	An X.509 certificate identifying SS's manufacturer
Cert(SS)	An X.509 certificate with the SS public key
Capabilities	SS-supported authentication and data encryption algorithms
SAID	The secure link between SS and BS (the connection ID)
RSA-Encrypt(k, a)	Instruction to RSA-OAEP encrypt its second argument a under the key k
PubKey(SS)	The SS's public key, as reported in Cert(SS)
AK	Authorization key
Lifetime	A 32-bit unsigned number giving the number of seconds before AK expires
SeqNo	A 4-bit value for AK
SAIDList	A list of SA descriptors, each including an SAID, the SA type—primary, static, or dynamic—and the SA cipher suite

Table 3: Terms used in the PKM protocol authorization message exchange.

Privacy and key management:

The Privacy Key Management protocol illustrate confirmed the SA data within Base Station and Subscriber Station. This protocol contains 2 or 3 message exchanges within BS and SS. BS utilize original optional message, and forcing to re-key. Alternatively, the SS specifies the law by forwarding 2- message, besides the BS replies within third message.

[Message 1:

BST → SST: SeqNum | SAID | HMAC (1)]

Message 2:

SST → BST: SeqNum | SAID | HMAC(2)

Message 3:

BST → SST: SeqNum | SAID | OldTEKs | NewTEKs | HMAC(3)

BST(Base station) does not utilize Message-1 until it needs to update SA data or generate a latest SA. By enumerate a value HMAC (1), it permits the SST (subscriber station) to discovers fraud. SS make uses of Message-2 to appeal SA frameworks.

SS should install SAID of the SAIDList either accreditation protocol or from Message-1 with accurate HMAC(1). Subscriber Station produces different Message-2 for each and every data Security Association (SA). It Includes the number of HMAC (2) to access Base Station to detect fraud.

Whether HMAC(2) is active and also Security association identifier (SAID) recognises one of the Subscriber Station SAs, Base Station prepares SA by using the Message-3. The Old TEK number doubles Security Association's operating limits over time NewTEK value determines the argument values to be used at the end of existing TEK. Triple Base Station Encryption for Data Encryption Standard latest and old TEKs below the authority of SA KEK, by using (electronic code book) ECB mode. Normal does not set TEK production requirements. Computing the HMAC value (3) allows the SS to detect fraud.

The allowable HMAC value (2) authorizes Base Station (BS) to Subscriber Station (SS). Two speculation supports this strategy:

- Utmost the Subscriber Station can disassemble the AK of the authorization protocol conveys to Message-3 as well as
- Authorization Key is unexpected.

The authorization protocol does not accept similar verification pattern of SS to BS; To be sure to adjust the values of HMAC (3) and HMAC (1) reveal only the certain group of the AK value accepted by Subscriber Station in Message-3 is designed Messages 1 and 3 of key management.

Encryption process:

Data Encryption Standard with cipher block chaining (DES-CBC) encryption working over payload phases, including explicit MPDU format, but not MPDU CRC format or GMH, as shown in below picture. The MPDU GMH conveys 2 fragments showing file for Traffic Encryption Key (TEK) is utilized. It did not carry the installer vector to start the Cipher Block Chaining mode. To compute the starting vector of MPDU format, 802.16 of IEEE module encryption X-ORs and the SA expression to begin with the help of content of the Physical layer sync field from the latest GMH.

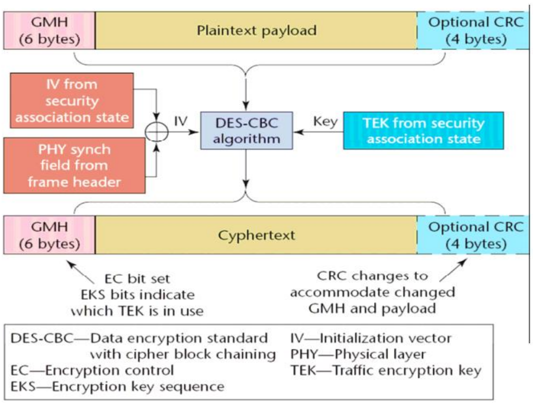

GMH (6 bytes)
Plaintext payload
Optional CRC (4 bytes)
IV from security association state
PHY synch field from frame header
IV
DES-CBC algorithm
Key
TEK from security association state
GMH (6 bytes)
Cyphertext
Optional CRC (4 bytes)
EC bit set
EKS bits indicate which TEK is in use
CRC changes to accommodate changed GMH and payload
DES-CBC—Data encryption standard with cipher block chaining
EC—Encryption control
EKS—Encryption key sequence
IV—Initialization vector
PHY—Physical layer
TEK—Traffic encryption key

Figure 8: 802.16 encryption process [12]

Since SA key vector implementation is permanent and socialize about its TEK, and Due to PHY sync area is highly recursive and unpredictable, the MPDU beginning or initialization idea also assumes.

802.16e of IEEE does not issues authenticity of the data.

802.16 security analysis of IEEE:

Various bugs endure in 802.16 security of IEEE.

Wireless MAN Threat Model:

Security risks spreads to both Physical layer and Media access control layer of IEEE 802.16e. Due to 802.11 security of IEEE performs entirely at MAC layer, it did not able to secure across PHY layer attacks.

The most common risks appear from the water torture attack, in when the attacker conveys a sequence of frames to detach the battery of receiver. One more risk requires an intruder, who refuses to work for all parties. Because the available strategies to prevent PHY level attacks are not enough to fit the rating focus only on MAC layer risks.

Advancement of 802.16 from fixed, line of vision, multipoint spot, high bandwidth system to lower bandwidth system, near the line of vision, and in the upcoming future, a cell phone attack, expand the rate of risks for end users. Threats is opposition to the first level, 802.16-2001of IEEE, needed that the enemy actually set off an attack system within Subscriber Station and Base Station and have ability to handle at approximately high bandwidth of 10 to 66 Giga Hertz.

The basic level of IEEE 802.16a introduced a low bandwidth performance, lowered the efficiency of the wireless circuit and PHY deployment issues. Networks Methods in 802.16a of IEEE implements latest safety considerations, existing security measures did not implement well, such as reliability of the upcoming bound of the network mesh node.

Attaching portability layer with 802.16e security creates the Intruder's life span much facile. Intruder's native area is rarely very restricted, creating administrative communication further at risk for 802.11 of IEEE. This require to handle a safe and secure circumstances at the same time Subscriber Station is on the move you walk through the BSs introducing new disabilities.

Various threats are common to any broad band channels. Whereas usage of radio in IEEE 802.16e, anyone can able to have a well arrange radio receiver put up block communication transfer through a file broad band medium. The composition should describe the method of discretion.

Developers of 802.16e deteriorate to refer one more risk: anyone who has been properly placed and repaired the radio sender have able to create a wireless station. Due to this weakness, the Intruder might fabricate latest parameters and apprehend, amend and retrieve frames works from certified organizations. Hence this pattern should impart a file for data reliability method.

Intruder might able to retrieve an efficient frame, which has been previously transmit was consistent. Intrusion and scope can permit the intruder to transmit with 2 authorized members who are unable to commune directly with one another, and rearrange and select further frame works. Hence, the pattern should find forge frames efficiently.

Inadequacy of explicit exposition:

The Ultimate impressive idea about the 802.16 of IEEE pattern is its loss to clearly define SA authorization, which means that has not ever received similar application that SA is receiving.

Threats to SA apply directly to authorization SA, so these failures may undergo to issues.

For Instance, the South African government not at all separates 1 example of approval of SA from other, leaving out rule open series to retrieve the replay attacks. Additionally, certified SA did not involve Base Station partnership, so Subscriber Station could not differentiate valid warranty of uncertified BS. Even though hidden BS specification through the user may covetable, hidden it from SS secure key control and encryption from securing the Subscriber Station (SS) from re-attacks and frauds.

These creates a connected issued to SA information. Since SS cold not split the re-authorized authorization by SA, either cannot detect or reused SAs. Encryption Strategy is hence unsafe to attack the intruder by reusing the encipher key.

The secure process to fix the threats of re-attack is to generate arbitrary value from Base Station and Subscriber Station to approval of SA. Searching for facts on either sides can secure donations. Verified BS ID removes risks posed to SS due to asymmetry of warranties.

Awareness to reattack also arises from the data SA definition. Normal treats two-bit key identifiers such as ring buffer, permitting the Intruder to minimize reuse Traffic Encryption key. Inventors must increase pattern key designated the memory to permit as much as possible key IDs to feasible transmitter by a very huge amount of AK life. Because Authorization Key could last long up to seventy days, and TEK life span could shorten up to 30 minutes, SA information could absorb until 3,360 TEKs with Authorization Key life span, needed to SAID growth space from 2 to 12 bits at least.

These problem arise the question familiar to whether TEK must run out. At the current rate, TEK expires after adjustable time. While it is absolutely inevitable, It is not adequate. Automatic Traffic Encryption Key life span of IEEE 802.16 is partial day, and rate allows a utmost Traffic Encryption Key time of 7 days. this values can accompany to issues.

Recollect that 802.16 of IEEE, for encryption we utilize DES in CBC mode. Due to usage of 64-bit block size DES – i.e., this operates on data blocks of 64 bit to generate every decryption or encryption effect. First theory is such that the Cipher Block Chaining mode utilizing a block cipher with n-bits forgets its own security follows operating on $2^{n / 2}$ blocks having similar encryption key[9]. Average rating of 6.36 Mbps generates 64-bit blocks of 2^{32} in half day; a standard 455 Kbps rating generates 64-bit blocks of 2^{32} in the recommended allowance of 7 days. Whether the rate of data is average surpass what is permitted in the lifespan framework position, the usage of encipher system is drastically reduced.

Requirement of mutual authentication:

The need to reassure both most apparent error of 802.16e of IEEE security pattern having a absence of Base station certificate. The one and only way to secure the user from either fabrication or re-attack is to restore a verification system with a strategy that provides approval for both. Two-way authentication is needed for all radio channels; reducing cable costs converted to guaranteed administration costs.

Authorization vulnerabilities:

Risk of authorization in line with SA's fragile pattern authorization, the Private Key Management authentication procedure that controls to be in danger.

The lack of IEEE 802.16 design of Base Station certification methods in Subscriber Station depart from, Private Key Management (PKM) protocol unsecure fabrication attacks. In a forgery attacks, SS could not authenticate any authorized data these was accepted and generated through any authorized Base Station. Base Station creates protocol authorization that conveys to SS applying public information Utterly, therefore any fraud BS could produce a file for the answer. Requires Subscriber Station authorization in BS can remove this risk.

Authorized protocol puts the SS under attack again. An easy process to overcome this types of attack for demanding that Subscriber Station create uncertain provocation in Message-2 of authorization protocol, along with BS to challenge province that restores authenticity to the SS.

A related problem is the failure of protocol to allow participants to separate a single example of a protocol from another. These would be principle as 802.16e of IEEE makes it easier to navigate and portability. With the help of swapping arbitrary values in public, Attendants may peculiarly finds a example of protocol such 4 tuple <BS's, SS's verified ownership, random public BS number for its example, random public SS number for its example>. Attendants might operate type of information to bind key management in the terms of the protocol in the context of the authorized authority. Authentication protocol identifies major Authorization Key-related issues. The procedure did not set needs for generating of AK, or for further usage takes arbitrary generation i.e., Authorization Key is chosen utilizing a consistent distribution of opportunities in memory of 160-bit cables.

These standard must create these type of point to clear. Some weaknesses exist because BS is addictive all segments in Authorization Key. these usual pattern defines Subscriber Station should hope that BS every time produces that latest Authorization Key secretly splits from entirely all AKs generated by every BS. It also defines that a random Base Station value produces should be finished - whether it shows great difference , it can reveal AK along with every TEKs. The most secure pattern can calculate Authorization Key with pieces of either donor organizations - for instance, AKey = HMAC-SHA1 (BS AK, a arbitrary value produced by SS). Comprehend the random public number produced by the Subscriber Station in the Authorization Key merger will confirm that its keys are new in SS.

Eventually, the procedure needed certificates be provided securely – i.e., there is no third party has to be involved and also must have distinct private and public key pairs are verified to utilize common MAC address. Whether this circumstance was not reach, every party can pretend to be a builder of other. The description should clearly state its assumption that all verified MAC addresses are different.

Issues with authentication protocol stand out tragic error of the 802.16 security of IEEE pattern. Management and encryption keys for IEEE components the safety of 802.16 does not guarantee the safety of both are subject to the validity of the authorization protocol. Here error indicates that having security capabilities need not be transmitted from one condition to other lack of having much attention.

Key management failures:

The deterioration of its authorization agreement stated that it does not matter if the IEEE 802.16 key protocol is precise or not. Anyhow, whether the authorization principle is ensued for pattern bugs fixed, issues in key management protocol will still sabotage security.

The Ultimate crucial key management protocol is its usage of Traffic Encryption Key sequence space. These protocol determines every TEK with a two-bit sequence number, binds up the sequence number from three to zero in all four racks. The usage of a sequence number protocol to separate messages to set it up again. If the iteration or replay is successful –Another time there is nothing in these protocol that accepts the Subscriber Station to identify this type of attack – The reusage of encryption by TEK and the start-up aim is on encryption, which automatically on both subscriber data and traffic Encryption key.

The definitive aborts to stated that TEK appear at random produce using the same distribution opportunities along with cryptographic quality number random generator. Due to encryption process needs this condition, the standard have to command you peculiarly.

Equivalently, the key distribution strategy does not attempt Traffic Encryption Key proof of burn. This is definitively inevitable in multicast, however not unicast. Also, you use keys to plan mix up the Subscriber Station uncertainly in the Base Station-provide TEK easily to accurate this issue.

Eventually, to overcome replays from following across the key management protocol, the standard could links communication to a specific protocol detail.

Data protection flaws:

Society apprehend that Data Encryption Standard fails to provide stable data privacy. The data protection system has a problem with more serious problems, however.

The failure of the scheme to defend against interference or retaliation, the two most serious risks to any wireless data protection system, is the most serious of these issues. Like IEEE 802.11 Wireless Secret compliance law, data protection system does not protect against fraud. Encryption only protects WMAN channel; did not secure the channel from address, Nevertheless by someone without having the encryption key.

The contract also specifies a crucial error at the time of usage of encryption. 802.16 security of IEEE uses Data Encryption Standard in CBC mode. CBC mode essential arbitrary start aim to protect the scheme [9], yet IEEE 802.16 utilize unpredictable boot direction. Fixing this issue requires individual production for every start-up frame by frame at the same time installation in re-paid line. Despite this access help to encryption of output, there is no another opportunity.

A way forward:

Ongoing activities for IEEE 802.16 security provided a chance to label common security problems. Upcoming and planned security designer methods share five main objectives:

- Use AES [10,11] as the first encryption. Use the present understandable mode performance, including the antidote to CCM (cipher block chaining MAC).
- Introduce a potent or dynamic based authentication system in EAP (Extensible Authentication Protocol) [12].
- Implement Security association (SA) accreditation as a first-class idea within the specified method.
- Primitive traditional attestation or authorization and key management.
- Allow for cost-effective reassurance at the time of roaming.

The Inventors have comprise few security methods are 802.16e and can deal with other bases standard default security before completion of IEEE 802.16d. All changes should be checked for security the social initial to the agreement of the revised accustomed.

New data protection strategy:

Amendment of IEEE 802.16 security freshly acquire AES-CCM i.e., AES in CCM mode, as a new data link cipher. CCM[13] incorporates encryption mode to data privacy with CBC-MAC for data authentication. Therefore, the accurate usage of AES-CCM utters to basic lack of a actual data protection system — the absence of data attested.

The Inventors select AES-CCM for a diversity of purposes, as well as its usage in IEEE 802.11i and upcoming testing. NIST in the US specified that CCM would be the accepted option for performing of AES. CCM secure related information, permitting the encipher system to secure GMH. There are no archived items to claim assemble by CCM.

AES-CCM essential to the sender to create an a unique instant, which is a randomizer for each packet encipher. Compatible with IEEE 802.11i standard, IEEE 802.16 security comprise packet number for each MPDU to secure the uniqueness of each and every instant. The recipient is proactively receiving duly removed packets beneath AES-CCM and have a cardinal in the packet that is accumulating.

IEEE 802.11e security also enumerates Advance Encryption Standard in ECB mode for re-operation set the 3-DES triple folding key to the privacy and key management protocol. A prominent choice would be NIST's Advanced Encryption Standard key-wrap algorithm[14].

Extensible Authentication Protocol (EAP) validation:

The task team considered two EAP-based options how to prove authenticity. The first is using IEEE 802.1X on move EAP messages. Company groups declined this phase as 802.1X of IEEE encapsulates Extensible Authentication Protocol messages as evidence independent, who thinks the data link is fully functional exists - false assumptions of any wireless method before the connection is stopped. The second method installs Extensible Authentication Protocol messages instantly in to 802.16 of IEEE administrative frameworks. These method allows attestation at the time of initiation of the link. IEEE 802.16 security introduced two auxiliary PKM messages to sends EAP: PKM-EAP-RSP and PKM-EAP-REQ.

IEEE 802.16 security didn't specify reliability methodology, and Extensible Authentication Protocol phases to encourages the scope of wireless security of networks are remains a research area. However, Inventors are starting to talk more often accepted parameters[15].

Converting to the Native attestation and key management:

To free the traditional IEEE 802.16 security PKM, we can attach single field to Message 2 and 4 fields in Message 3, then count the file for Authorization Key by fresh way:

Message 1:

SST→ BST: certificate (processor (SST))

Message 2:

SST → BST: SST-Rand | cerificates (SST) |

Power | SAID

Message 3:

BST → SST: SST-Rand | BST-rand | RSA-Encrypt (Pub-Key (SST), pre-AKey) |

All Life | SeqNum | SAID-List |

Certificate (BST) | Sign(BST)

Table-3 describes the word used in above messages. Installing a computer in Authorization Key utilize the new process AKey = HMAC-SHA1 (pre-AKey, SST-Rand | BST-Rand | SST-MACAdd | BST-MACAdd | 160) generates new Authorization Key is about the same length as the current AK. Together with SST-Rand and BST-Rand in the outcome confirming SST and BST that the emerging Authorization Key is new, Nevertheless of the contributions of peers. Entering MAC addresses to get AK secure the key to this position of fellows, Together with nominal the length secure the fabrication from the attack of expansion. HMAC-SHA1 is used contrary to Vanilla SHA1 for the keys to Upcoming release — proof of design counter to attack hash function. These protocol fixes security breaches in attestation process.

To accurate important conduct errors, we propose to implement the SST-Rand | BST-rand and extend SeqNum to atleast 12 bits, attach a condition that you will never wrap:

[Message-1: BST → SST: SST-Rand | BST-rand |

SeqNum12 | MEANING | HMAC(1)]

Message-2: SST → BST: SS-Rand | BST-rand | SeqNum12 | MEANING | HMAC(2)

Message-3: BS → SS: SS-Random | BS-random |SeqNo12 | MEANING | OldTEKs | NewTEKs | HMAC(3)

Whether the SA information is unicast, we recommend the availability of TEKs rather than distributing it: TEK = HMAC-SHA1 (preTEK, SST-Rand | BST-Rand | SST-MAC-Add | BSMAC-Add | SeqNum12 | 160)

We aim to nominate such changes to the company group e.

Lowcost Roaming:

Proof of authenticity is an extravagant task, at the same its knowledge appears that it meets the demands of operation to cause requests, it requires lower attestation costs in addition to connecting with multiple BSs. With a voice call resettling, for Instance, ITU endorse that the time allying leaving one Base Station and renewing the context in another Base Station has certainly not exceeded 30 ms. Conversely, the assertion of defending the design of the protocol that BS does not participate in AKs or Traffic Encryption Keys; or else, conciliate on one Base Station puts Subscriber Station on all Base Stations they visit at a time the same time. Solving this problem requires more retrospective development, outside the IEEE 802.16 security. Algorithm programs evolves to label this issue persists in both IRTF and IETF.

Conclusion:

IEEE 802.16e is an emerging standard for hardware manufacturers and broad band wireless communication service provider as back-up approach to wired broad band connection or as efficient wireless Local Area Network average. During the execution of the concept, it was found to be possibly 802.16 at risk. However, that risk is a hypothesis, according to a paper review. Because of sequel, At the same time operator would supply definitive implements, it would be so proved that these risks identified and implemented in this concept really exist. Even then, buying one is still out of reach for most people. It really is different attacks made of paper have been described as actual exploitation we have a small door of chance afore the level arrive in the Industry, so that experimenter can assure its safety and procure it to the social use it, there are less security errors as hypothetical.

Future scope:

IEEE 802.16 security has the prospective to attain significant success on Upcoming Industry, Even though due to its security flaws probably hampered its acquisition. We have proposal to work within IEEE 802.16 security and Internet Engineering task force (IETF) to indicate the security vulnerabilities recognized here.

References:

1. IEEE Std. 802.16-2001, IEEE Standard for Local and Metropolitan Area Networks, part 16, "Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2001.

2. W.A. Arbaugh, N. Shankar, and Y.C. Wan, "Your 802.11 Network Has No Clothes," Mar. 2001; www.cs.umd. edu/~waa/wireless.pdf.

3. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," Feb.2001; www.isaac.cs.berkeley.edu/wep-faq.html.

4. "Weaknesses in the Key Schedule Algorithm of RC4," by S. Fluhrer, I. Mantin, and A. Shamir, Proc. 8th Ann. Workshop Selected Areas of Cryptography, Springer-Verlag, 2001, pp. 1-24.

5."Unsafe at Any Key Size," by J.Walker, Oct. 2000; http://grouper.ieee.org/groups/11/Documents/Document Holder/0-362.zip.

6. IEEE Std 802.11-1999, IEEE Standard for Local and Metropolitan Area Networks, part 11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification," IEEE Press, 1999.

7. Secure Hash Standard, Nat'l Inst. of Standards and Technology, Apr. 1995; FIPS PUB 180-1 http://csrc.nist. gov/CryptoToolkit/tkhash.html.

8. Data Encryption Standard (DES), Nat'l Inst. of Standards and Technology, FIPS PUB 46-3,

Oct.1999;http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

9. RSA Cryptography Standard, RSA Public Key Cryptography Standard #1 v. 2.0, RSA Laboratories, Oct. 1998,

10. "A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation," by M. Bellar et al,Proc. 38th IEEE Symp. Foundations of Computer Science, IEEE CS Press, 1997, pp. 394-403.

11. Advanced Encryption Standard (AES), FIPS PUB 197, Nat'l Inst.of Standards and Technology,Nov.2001,http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

12. "PPP Extensible Authentication Protocol (EAP)," by L. Blunk and J. Vollbrecht, RFC 3748, Internet Eng. Task Force, 2004.

13. D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," RFC 3610, Internet Eng. Task Force, Sept. 2003.

14. R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm," RFC 3394, Internet Eng. Task Force, Sept. 2002.

15. B. Aboba, D. Stanley, and J. Walker, "IEEE 802.11 EAP Requirements," Internet draft, work in progress, Jan. 2004.

16. Hassan Yaghoobi: 802.16 Broadband wireless access: the next big thing in wireless. Intel Developer Forum, Sep 2003.

17. Carl Eklund, Roger B. Marks, Kenneth L. Stanwood, Stanley Wang: IEEE Standard 802.16: A Technical Overview of the WirelessMAN™ Air Interface for Broadband Wireless Access, IEEE Communications Magazine • June 2002

18. Stevens Institute of Technology:Wireless Metropolitan Area Networks (WMANs) 802.16, 2003

19. K. Wongthavarawat, A. Ganz. "IEEE 802.16 Based Last Mile Broadband Wireless Military Networks With Quality of Service Support." Proceedings of MILCOM 2003. IEEE, 2003.

20. C. Wullems, K. Tham, J. Smith, M. Looi. "A Trivial Denial of Service Attack on IEEE 802.11 Direct Sequence Spread Spectrum Wireless LANs." Proceedings of the 2004 Wireless Communications Symposium. IEEE, 2004.

BIOGRAPHIES:

Voora Lakshmi Haneeja is pursing B.Tech. Computer Science and Engineering in Lovely Professional University.

Shaik Jasmin is pursing B.Tech. (hons) Computer Science and Engineering in Lovely Professional University