# Mobile Cloud Computing Cryptographic Scheme

[1]Vikram Patalbansi [2]Dr. G. Prasanna Laxmi

[1]*Research Scholar Pacific University, Udaipur India*
[2]*Faculty, Andhra University, India*
[1]vikrampatalbansi14@gmail.com,
[2]prassnalaxmigandi@gmail.com

***Abstract***
***The ubiquitous network like Mobile Cloud Computing (MCC) provides the high quality of wireless services depending upon the wireless communication system network security level. And so many researches are carried out by the researcher on security algorithms for wireless communication system constructed in different network reliability. In our proposed thesis paper, on a theoretical basis, we developed the theory of MCC Security Layer Protocol security system in which we used the cryptographic hash function SHA-256 to generate a private key for entities, RC5 encryption, and decryption algorithm, Temporal Key Integrity Protocol (TKIP) generating a dynamic sequential key and CRC-32 checksum to detecting the error in our packets. The MSLP uses the stored symmetric secret key calculated on the basis of the Diffie-Hellman Key sharing scheme to generate keystream for cryptography functions. The secret key stored in the device's filesystem our database prior to the deployment on Mobile Cloud Computing and remains the same throughout the session of communication. These systems use the dynamic initialization vector to avoid reply attacks and message integrity code calculated on source and destination devices addresses and actual frame contents. In the proposed thesis paper we analyze the security measures at MSLP level and before transmitting information over the mobile networks, the information is encrypted in the form of frames and at the physical layer, this frame converted into its equivalent radio signals.***

***Keyword*: Mobile Cloud Computing, mobile network security, wireless signal security algorithm**

## INTRODUCTION

The Mobile Cloud Computing (MCC) consists of individual mobile phone, laptop, or any other electronic devices which are connected with cloud server via the cellular network. Both the entities mobile devices and cloud server shares resources and information to each other over the wireless communication. The need for security in MCC, which arises from the transmission to receiving of secured information. Due to the broadcast nature of the wireless radio channels, anyone can monitor or access wireless communication. In addition to the myriad vulnerabilities of the conventional wired networks, the wireless networks also has a host of the other vulnerabilities associated with the use of radio communication and mobile endpoints. The packets are transmitted over the air link, which makes it relatively easy to eavesdrop, intercept them, inject malicious payloads or launch Denial of Service (DoS) attacks. [1]Though the cloud communication services providers offer security protection as part of its service and must also take measures to ensure data and information are secure. The fundamental factor defining the success of any new information computing technology is the level of security, it provides to the user. The service provider must fulfill security requirements like confidentiality, integrity, and availability to protect the information in wireless communication.[4]In general, most wireless network receivers devices including all IEEE 802.x protocol compatible devices start to accept messages in the air once a synchronization header (preamble) is detected. They stop receiving messages based on a frame length byte. If collision occurs during the reception of the header, nothing can be received. So to avoid such kind of difficulty proper packet encryption techniques must be used in Mobile Cloud Computing.

## PROPOSED THEORY

[3]In Mobile Cloud Computing (MCC) security issues are divided into three levels viz. Security of mobile devices/terminals, Security of wireless communication channels, and Security of cloud infrastructures. Here in this section, we will discuss security on wireless communication channels. Using Mobile Cloud Computing, mobile users communicate with the cloud servers with the help of communication channels or wireless interfaces. There are lots of possibilities for attackers to breaks the traditional security arrangements using encryptions techniques or authentications techniques. Because most of the attacker are used to with this techniques and by doing R&D, they can easily do security break up in security arrangements likes access control attacks, confidential attacks,

integrity attacks, authentication attacks, and availability attacks.

[5]To achieve all of the above objectives, we propose our self-defined protocol architecture called MCC Security Layer Protocol (MSLP). Our MSLP provides a multi-layered security framework designed during chip manufacturing and mounted on-chip with security protocol for encrypting and decrypting mobile devices information. The chip mounted information is not malleable with unique identification configured with debug read-back feature disabled by preventing reverse engineering with standard debugging tools, which is a common vulnerability.

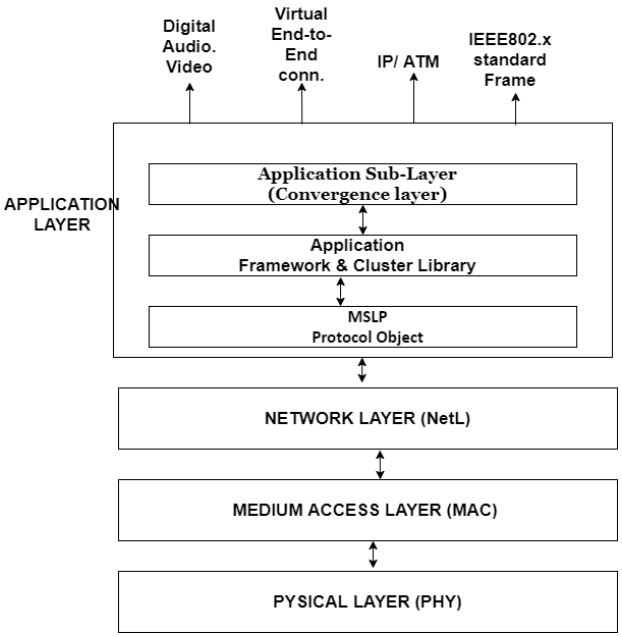



Fig. 1 MCC Security Layer Protocol(MSLP)

The working of the MCC Security Layer Protocol is a little bit the same as the TCP/IP protocol layer in the internet network. Here we are using our protocol in Mobile Cloud Computing to fetch information from cloud servers for our electronic mobile devices over cellular (mobile) networks and vice versa.

[15]The main aim of this protocol layer to provide security to information over wireless communication. From mobile devices, we want so many services like video, audio, photo, digital contents files, etc. For these services we need different types of security mechanisms depends upon the number of bits in the frame.

A) Application Layer: The application layer provides the interface to the outside world to takes input from the user. The application layer divided into three logical sub-parts.

i) Services: For mobile devices, we require lots of services like video/audio digital signals transmitted between mobile devices and cloud servers via cellular networks. The ATM services provide logical distribution of frequency spectrum over network slices and IP service provides internet service by creating IP datagram. And using IEEE 802.x standardization, MSLP also supports Wi-Fi, wi-max network by generating its compatible frames.

ii) Application Sub-Layer (Convergence Layer): This sub-layer maintains the quality-of-service (QoS) of the services provided by the mobile network.

iii) Application Framework and Cluster Library: This sublayer performs the functionalities the same as the presentation layer in the OSI reference model. Whatever information entered by the user through the application layer, this sub-layer first converts into machine dependant format i.e. binary digits, and complied it by using an in-built cluster library. After cross-checking in the proper format, this sub-layer generates frames or packets.

iv) The MSLP Protocol Object interacts with Mobile Devices' authentication application and reads the secret key generated by the cellular network on the basis of IMSI, IMEI (or MAC address in case of electronic devices apart from Smartphone, etc.) fingerprint, virtual smart card and universal integrated closed circuit (UICC) by hashing with random number generated by registration center of Cellular network. We explained this entire concept in our previous paper. That secret key is denoted by VIdent. The MSLP Protocol Object read this secret key and use it for encrypting our frame. The generation of VIdent explains in the following figure

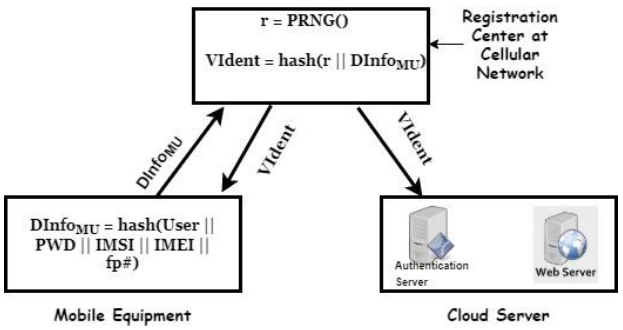



Fig.2 Generation Pair-wise Transient Key VIdent

B) The Network Layer (NetL) in our protocol MSLP provides the functionalities of the creation

of packets or frame compatibles with wireless network configuration. With respect to network configuration, the network layer generates frames.
Also, the network layer stores the routing table information of the transmitted and received frames by broadcasting router request message and processing received route reply message. It also established logical connections between mobile devices and cloud servers by generating session keys and acknowledging communication at both ends.
At this Network Layer, we can also apply the network security process on frame coming from Application Layer by implementing through Internet Protocol Security (IPSec) which is comes under Internet Engineering Task Force(IETF) standardization. It also generates a frame in conjunction with our protocol MSPL network layer. IPSec functioning over network architecture and end-users and its application no need to configure in any way. The encryption processes are invisible at both end and encryption of packets performs independently and transmitted through the IP network over the cellular network.
C) Medium Access Layer (MAC): As per standardization of IEEE, every network device whether they are used in the wired or wireless networks, must to follows unique identification worldwide known as MAC address or we can say that physical address of electronic mobile devices. The MAC addresses are implemented in electronic mobile devices at the time of the manufacturing of devices. The IEEE is a universal registration authority of electronic devices and any devices addressed can be cross-checked online according to wireless network configuration. As per our MSPL protocol standardization, the MAC layer is responsible for its own security processing, but the upper layer Application Layer logical subparts of MSPL protocol object reads the unique authenticated key VIdent with the help of authentication application and this authentication keys determine encrypting key to frame or level of security to use. This authenticated key VIdent is an active network key because as soon as mobile devices disconnected from cellular networks or cloud servers, the authentication application automatically deallocates memory occupied by it. Apart from this, the MAC layer performs the jobs of error detection or correction for the frame during transmission and receiving of the frame. For encryption, decryption, error correction and decryption of the frame, some inbuilt logical circuit is embedded into MAC layer for enhancing functionalities of MSLP protocol, and also WAP2 protocol is a technical standardization to access the information over the mobile wireless network is embedded into MAC layer for generating IP datagram for internet communications. The main tasks of the MAC layer are that creates a logical mapping of data to Physical layers, multiplexing, channel scheduling, header compression, packets reordering, retransmission of lost packets, all cryptographic protection to access stratum signals including integrity and confidentiality, etc.
D) The Physical Layer: [10] The cellular networks are composed of different – different Radio Access Network (RAN) to form Evolved Universal Terrestrial Radio Access Network (E-UTRAN). In Mobile Cloud Computing, electronic mobile devices like smartphones. Laptop etc. are connected to cloud servers over cellular networks' internet with help of intermediate E-UTRAN consists of a set of base stations overall areas known Evolved Node B (eNodeB) which modulates and demodulates radio signals to communicate with mobile devices or user equipment (UE). The eNodeB or cellular network base station acts as a relay point to create and send IP packets to and from the internet connection. The main task of the Physical layer in our MSLP protocol suite is to establish a connection with the eNodeB of mobile devices. It converts the upper layer frame or packets into equivalent radio signals to transmit over RAN using a network adapter that gets implemented over it. The over the air interface, MSPL protocol performs mainly two functionalities using two logical operational planes viz i. The user plane ii. The control plane. The user plane transmits user data likes voice communication, SMS, application traffic. And the control plane is providing all signaling communication require for mobile devices to connect with eNodeB or mobile network base station (BS). According to 3GPP, the cellular network working protocol is divided into two logical layers as a) Non-Access Stratum (NAS) and b) Access Stratum (AS). The Access stratum is all about communication between mobile devices and radio frequency (RF) channels. The NAS consists of all non-radio signaling traffic between mobile devices and cellular network infrastructure. Overall this different layer, the Physical Layer of MSPL protocol suite is responsible for to setup, maintain and terminate the air interface connection

between the mobile devices and mobile (cellular) network different entities by performing various control tasks such as broadcasting system information, establishing a connection with eNodeB, transmitting paging signals to the various base station, perform authentication with registration center of cellular network, bearer establishment and transferring Non-Access stratum message

SECURITY ARCHITECTURE:

Step 1) In the wireless communication security mainly depends upon cryptographic techniques are used in the MAC and Application layer. But we are also providing security measures on the physical layer as well as over Radio Access Network. So that due to eavesdropping in wireless communication, our information must be secure in an encrypted form.

Our layered protocol MCC Security Layer Protocol (MSLP) is built on the basis of IEEE 802.15.x standardization and provides cryptographic protection among various mobile networks and its entities. The upper layer Application Layer provides an interface to the mobile user and converts it's inputted information in mobile devices hardware configuration compatible format. Then the Network layer, MAC layer, and Physical layer support necessary operations required for transmitting information over the wireless communication network. For the secure end – to – end wireless communication over Mobile Cloud Computing (MCC), we will use the dynamic encryption technique ensuring that for each session between mobile devices and cloud server, the information in the form of the frame is encrypted with randomly chosen encrypting keys with the help of an asymmetric key algorithm. [11]Here we are using Diffie-Hellman key exchange methods to exchange encrypting keys and Wired Equivalent Encryption (WEP) protocol based on RC5 PRNG (Ron's Code 5 Pseudo-Random Number Generator developed by Ron Rivest to encrypt the frame between mobile devices and cloud server over a cellular network. The frames or packets are the minimum transmission entities over the data rate of transmission that are kept constant. The source bit rate can be different packet by packet.

Step 2) Traditionally for encryption procedure the sender and receiver devices share the symmetric key (i.e. public key) and the kreyvium encrypts the data on the basis of the sender public key and then transmits the data along with public encryption key to the receiver. At the other end, the receiver decrypts the data with the help of a public key that has been sending by the sender along with cipher data. The main disadvantage of this method is that due to eavesdropping, the third party or hacker hacked the encrypting key at once during the transmission session and all the data gets decrypted by them. Hence to overcome these problems, we have to use the Diffie-Hellman key exchange protocol to shared secret keys between two entities over Mobile Cloud Computing. The information exchange between the sender and receiver is public means can be hack by anyone but cannot be decrypted because encryption and decryption are performed by secret keys which are calculated with help of Diffie-Hellman Key Exchange protocol. Here we will use asymmetric encryption (i.e. public and private key concept) to exchange the secret key between users.

During registration of mobile devices over the cellular network's registration center (RC), the RC generates key VIdent and VIdent shared with mobile devices and cloud servers and stored in their memory. VIdent is globally known by all entities of Mobile Cloud Computing.

Step3) To generate the private key of the mobile devices (UE) in a random manner, here we are going to use cryptographic Secure Hash Algorithm-256 (SHA-256) which produces hash values that are hard to predict from the input. The SHA-256 algorithm is free to use publically and many high-level programming languages having in-built libraries to implements in our use. By apply SHA-256, the sequence of random numbers generated is correct and unpredictable on the basis of inputted values.

Now in mobile devices, authentication application gets installed which is provided by the cloud service providers to get cloud service from them. First mobile user login with authentication application by inserting a valid username and password. The mobile devices also having unique parameters such as IMSI, IMEI (in case of laptop and iPod MAC address according to IEEE standardization), Universal Integrated Closed Circuit (UICC) issued by the cloud service provider only to its customer and its identity is unique worldwide and it is like a hardware chip embedded into mobile extensible hardware slots and using biometric module existing into mobile devices tke the valid user finger impression(fp) and with the

help of Fuzzy extractor function, we can generate its respective string parameter(fp#) in a random manner..

All these parameters like user, pwd, IMSI, IMEI, UICC, and fp# assuming as seed value into the hash function to generate the required value as a seed value of the user of the mobile device at that session only to input into SHA-256. For every new session, we have to generate new seed values

Consider

$DInfo_{MU}$ = hash(user || pwd || IMSI || IMEI || fp# || UICC)

The essentials elements of any pseudorandom number generator (PRNG) are seed value and a deterministic algorithm for generating a stream of pseudorandom function (PRF) to produce the required private key of the user. Here we are using algorithm Secure Hash Algorithm-256 (SHA-256) and $DInfo_{MU}$ .

.

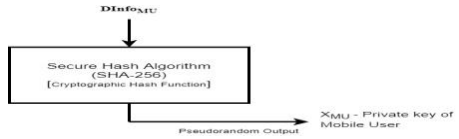



Fig.3 Private Key generation of Mobile user

$X_{MU}$ = SHA-256($DInfo_{MU}$);

Similarly, we can generate the private key of Cloud Server (CS). Also, authentication application is installed on a cloud server to take username (userCS) and password (pwdCS) of valid cloud server administrator and MAC address of cloud server (approved by IEEE registration authority and it's can be online cross-checked on IEEE), IP address of cloud machine (IP) to get internet services which are factory programmed and act as a unique identity and port number (PORT) over which application(web) server is running in cloud server.

**$DInfo_{CS}$ = hash(userCS || pwdCS || MAC || PORT || IP)**

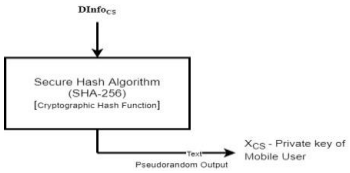



Fig.4 Private Key generation of Cloud Server

$X_{CS}$ = SHA-256($DInfo_{CS}$);

Both the value YMU and YCS are globally known to every entity of Mobile Cloud Computing and are public keys of mobile devices and cloud servers respectively.

Now consider a prime number 'q' and assume that 'α' such that it must be the primitive root of the q and α<q. Both the values 'α' and 'q' mutually decided by both the end devices and publically known to all entities.

Hence by using Diffie-Hellman Key Exchange formulas, we can derive the public key of both Mobile device and Cloud Server as follows.

1. $Y_{MU} = \alpha XMU \bmod q$……for Mobile Device

And

2. $Y_{CS} = \alpha^{XCS} \bmod q$……for Cloud Server.

Both private keys values $X_{MU}$ and $X_{CS}$ of mobile devices and cloud servers respectively are kept secret and mobile devices and cloud servers share public keys values $Y_{MU}$ and $Y_{CS}$ to each other.

Then we have to go to calculate packet secret key ($SK_M$ ) when mobile devices are the sender of the packet using the Diffie-Hellman Key Exchange formula.

$SK_{MU} = (Y_{CS})^{XMU} \bmod q$ ….Secret key for packets at mobile devices during sending of packets.

$SK_{CS} = (Y_{MU})^{XCS} \bmod q$ …. Secret key for packets at cloud server during sending of packets.

According to the Diffie-Hellman Key Exchange protocol or rules both the secret key at both the end must be equals. This is a basic assumption in our proposed methodology. i.e.

$SK_{MU} = SK_{CS}$ ( using Diffie-Hellman Formula)

Both the secret values $SK_{MU}$ and $SK_{CS}$ are inputted into RC5 Encryption and Decryption protocol, which is a factory-fabricated and programmed into Medium Access Layer(MAC) of MSPL protocol to encrypts the each and every packet and perform error detection on each packet.

The following protocols and algorithms are used in encrypting and decrypting of the packets coming from the upper layer of MSPL protocol.

1. The Temporal Key Integrity Protocol (TKIP): The TKIP protocol suite of algorithm or specification is wrapped over existing encrypting protocol in mobile devices of wireless network communication by upgrading its capabilities without any hardware modification. The TKIP is pre-processing steps before RC5 protocol encryption. The new TKIP protocol's TKIP Sequence Counter (TSC) generates Dynamic

Initialization Vector (DIV) which is used for encrypts each data packets with its unique encryption with strong values and for next packets, DIV keys get updated each time and seed into RC5 encryption algorithm protocol. To increase the key strength values, TKIP also supports the following algorithms.

i. Use of Message Integrity Check (MIC) along with CRC-32 to provides better integrity to packets. The MICHAEL MIC is not just a function of the data of the packet. It also depends on the sender's MAC address, the receiver's MAC address, and the priority of the packet, as well as the PTK( pair-wise transient keys). Here in our protocol VIdent – pairwise transient keys is already calculated at the time of mobile device registration at the cellular network. MICHAEL is designed to avoid the iterative guessing and bit flipping.

ii. For every packet, the key mixing function is executed to increase cryptographic strength.

iii. The TKIP Sequence Counter (TSC), expand the Dynamic Initialization Vector (IV), and key ID fields to 8 bytes and also DIV can be expanded up to 8 bytes which are further used in hashing function cryptography. It is useful in avoiding the replay attacks because every packets sequence counter is different when replay attacks are attempted.

iv. A re-keying mechanism to provide new key generation after every 1000 packets.

v. The MICHAEL is a method of computing the MIC (Message Integrity Check) that uses no multiplication but just shifting and adding operations to generate short check word. The MICHEAL MIC calculation based on the entire frames, not on individual fragments of the frame, The MICHEAL combines together all the bytes in the message frame and generates 8 bytes check value called as MIC (Message Integrity Check) which is placed at end of the frame along with original message before sending to receiving devices. The MICHEAL MIC is computed using a special on the reversible process and combing with the secret key of the mobile devices. The PTK (pair-wise transient keys) i.e. VIdent already known by mobile devices and cloud servers. MIC computation includes packet destination and source device's MAC addresses to protect against redirection attacks and added source validation mechanism. It is added at the rear of the frame as a safeguard to unauthorized alterations. The only valid receiver knows the pairwise transient key VIdent, can be recomputed its real check value MIC. Hence MIC is a type of message authentication code used to detect packet forgeries.

vi) Dynamic Initialization Vector (DIV): The TKIP Sequence Counter (TSC) assigns a packet sequence number to MIC and dynamically increments to new sequence value for next packets and the same sequence value cannot be repeated during the entire session. The range of the sequence number shared between sender and receiver and beyond it all packets with out of range sequence number discarded.

2. RC5 Encryption Algorithm: It is a symmetric key block encryption algorithm designed by Ron Rivest. It is much simpler, consumes less memory, and fast in computational operations like XOR, shift, etc. as compared to RC4.

The RC5 consists of three algorithms like key expansion, encryption, and decryption. All algorithms caries mainly three operational steps.

(a) Two's complement addition of word denoted by "+". This is modulo-2w addition.

(b)Bit-wise exclusive-OR (^) of words.

(c) A left rotation or left spin of words.

The rotation of word x left by y bits is denoted by x <<< y. The only lg(w) low –order bits of y are used to determine the rotation amount so that y is interpreted modulo w.

The RC5 is a block cipher and can perform cryptography on two words at a time. The RC5 can be defined and expressed as RC-w/r/b where w is word size in bits, r is a number of rounds, and b is the key size in bytes. The key size will vary from 0 to 255 bytes and the possible number of rounds will vary from 0 to 255. The RC5 block or word size will be 16 bits, 32bits, or 64 bits only. Hence RC5 uses 2-word block, then plain text block size can be 32,64 and 128 bits only

## THE PROPOSED METHODOLOGY

First, our assumption is that the secret key $SK_{MU}$ at mobile devices and the secret key $SK_{CS}$ at cloud sever are equal according to the Diffie-Hellman key Exchange Scheme. Hence $SK_{MU} == SK_{CS}$.

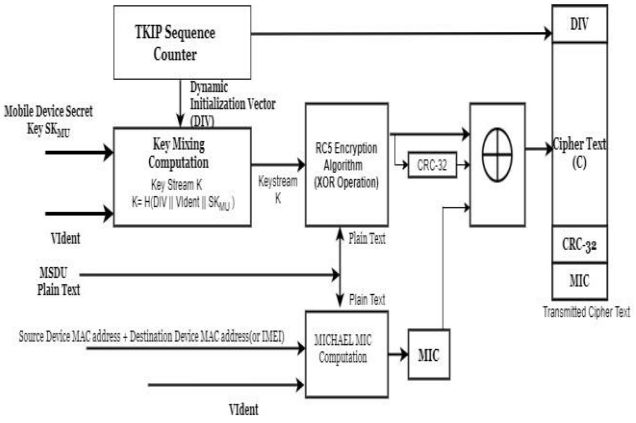
In any situation, both the secret keys do not share with each other over Mobile Cloud Computing (MCC) among any entities. The value VIdent is calculated by Registration Centre (RC) on the basis of parameter send by mobile devices and RC shared the same value of VIdent to the mobile device and cloud server and respectively both store this value in their memory file systems.

Here we can say that VIdent is a pair-wise transient key (PTK) between mobile devices and cloud servers. Whenever a connection is established between them, both devices shared MAC (physical) addresses of each of one to each other. In the case of a smartphone, we can consider IMEI code instead of the MAC address. Both the address denoted by $MAC_{MU}$ and $MAC_{CS}$. After connection establishment between the mobile device and cloud server TKIP Sequence Counter (TSC) generates packet sequence number i.e. dynamic initialization number (DIV) which is going to update its value for every MAC Service Data Unit (MSDU) packets. The range of DIV starts from any random number and finished at any random number. This range of DIV denotes by {r}.

At first, the sending device, we can say here mobile devices transmit this range in encrypted form to receiver device i.e. cloud server. Assume the following algorithm. For encrypting {r} we use the 3DES algorithm in the following algorithm.

| **Algorithm 1: Sending Range of Dynamic Initialization Vector.** |
|---|
| *Requirement :* |
| isAvailable(mobile device , mobile network,cloud server,TKIP_Sequence_Counter) |
| hasNetworkAccess(mobile device, cloud server) |
| *Procedure :* |
| **Role_Of_Mobile_Device** |
| const $SK_{MU}$,VIdent, $Y_{MU}$ |
| var {r} |
| {r} = $E_{YMU}(D_{VIdent}(E_{SKMU}(\{r\})))$ |
| CS ← $Y_{MU}$ ,{r} |
| **Role_of_Cloud_Server** |
| recv($DInfo_{MU}$) |
| const $SK_{CS}$ , VIdent,$Y_{MU}$ |
| var {r} |
| {r} = $D_{SKCS}(E_{VIdent}(D_{YMU}(\{r\})))$ |
| #database ← pointer { store ({r})} |

After executing these steps, predefined range of dynamic initialization vector(DIV) store in database memory of Cloud Server for further reference.




TIKP-WEP-RC5 Encryption at Transmission End

Fig.5 TKIP-WEP-RC5 Encryption at Transmission End

ENCRYPTION OF THE PACKETS AT SENDING END

Step1) The TKIP's TSC generates the Dynamic Initialization Vector (DIV) for a specific packet and passes to the Key Mixing Computation Function. Here also Secret Key of mobile devices $SK_{MU}$ which one calculated using Diffie-Hellman Key Exchange Scheme and Pair-wise Transient Key VIdent are also seed into this function and after calculation Keystream, K is generated.

K = H (DIV || $SK_{MU}$ || VIdent).

Step 2) In this step Source devices and Receiving devices MAC address and pairwise transient key VIdent are inputted into the MICHAEL MIC method along with plaintext (MSDU) coming from the upper layer of MSPL. After execution of the MICHAEL MIC method Message Integrity Code (MIC) is generated by adding all bytes in the MSDU. After this MIC code forwarded to the cryptographic hash function.

Step3) In the next steps, the upper layer plaintext (MSDU) inputted into the RC5 encryption algorithm. Also, keystream K which was calculated at step-1 is also inputted. RC5 is a simple and symmetric encryption algorithm with low memory requirements whose plaintext and ciphertext are fixed-length bit sequence with data-dependent rotational shifts. The key-expansion algorithm initialization S from the keystream K to fill the expanded key array S so that S resembles an array of S[0,1,……(t-1)] where t = 2(r+1) random binary words determined by K.

In our algorithm, each encryption and decryption function accepts two blocks of data either ciphertext and plaintext, and rotation shift or a number of rounds depends on the block of data.

| **Algorithm : Encryption of packets using RC5** |
|---|
| ***Input :*** Plaintext in two 32-bits variable A & B |
| Number of rounds (R) |
| Expanded key table S[] |
| ***Output:*** Ciphertext stored in variable A and B |
| ***Procedure :*** |
| A = A + S[0] |
| B = B + S[1] |
| var I; |
| for I = 1 to R |
| A = ((A $\oplus$ B) <<< B) + S[2 * I ] |
| B = ((B $\oplus$ A ) <<< A) + S[2 * (I+1)] |

Step 4) After encryption of packets, then on the basis of bits of ciphertext using the CRC-32 error detecting algorithm, CRC-32 checksum are calculated and will be added at the end of MPDU.

Step 5) All these three variables CRC-32 checksum, ciphertext and MIC code from MICHAEL MIC methods are seed into cryptographic hash function and compress into packets so that it can reduce the header size of MAC Protocol Data Unit (MPDU) to be compatibles with wireless protocol's maximum transmission unit (MTU). The packets after compression and cryptographic hashing will look like as follows.

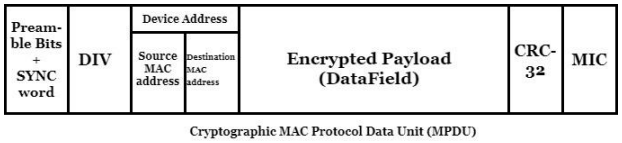



Fig.6 Cryptographic Packets

The MIC and CRC-32 values added at the rear position of MPDU and DIV at the front position of MPDU.

[14]Then these packets transmitted over the wireless networks after performing formalities over the physical layer of MSPL. The network adapter at the physical layer converts all these entire packets into its equivalent wireless signals and transmitted over cellular networks.

DECRYPTION OF PACKETS AT RECEIVING END

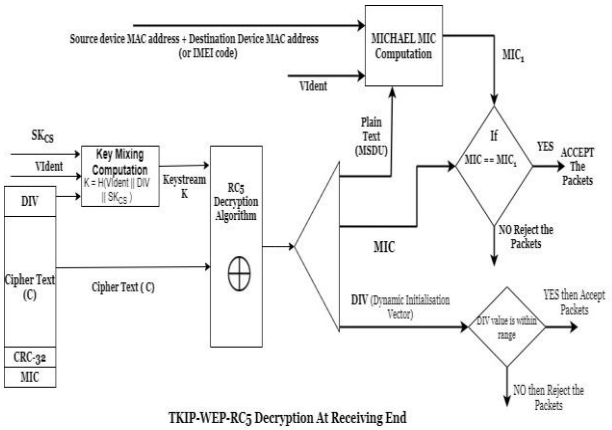



FIG.7 TKIP-WEP-RC5 DECRYPTION AT RECEIVING END

Step 1)Whenever encrypted signals received by the end device then the network adapter convert encrypted wireless signals into encrypted ciphertext packets at the physical layer of MSPL and then after synchronization and preamble procedure over the physical layer then this ciphertext frame transfer to MAC layer of MSPL. Here Packet decryption, validation, and error detection are performed.

Step 2) First DIV is separated from ciphertext and seed into Key Mixing Computation function along with Pair-wise transient key VIdent and Cloud Server Secret key $SK_{CS}$. Then after the computation of Key mixing function, the keystream K will be generated as it is the same value at sending or mobile devices because $SK_{MU}$ and $SK_{CS}$ must be the same by Diffie-Hellman Key Exchange formula.

Step 3) Then by using RC5 Decryption algorithm this ciphertext is decrypted as follows

| **Algorithm : Decryption of packets using RC5** |
|---|
| ***Input :*** Ciphertext in two 32-bits variable A & B |
| Number of rounds (R) |
| Expanded key table S[] |
| ***Output:*** plaintext stored in variable A and B |
| ***Procedure :*** |
| var I; |
| for I = R to 1 |
| B = ((B – S[2*(I+1)]) >>> A ) $\oplus$ A |
| A = ((A – S[2*I]) >>> B) $\oplus$ B |
| B = B – S[1]; |
| A = A – S[0]; |

Then all the values in Cipher text separated into four parts DIV, plaintext, CRC-32 and MIC. All these four values will be validated then packets are accepted.

Step 4 ) Validation of DIV.

| **Algorithm : Validation of DIV** |
|---|
| ***Input :*** DIV from ciphertext |
| Range of DIV {r} |
| ***Output :*** DIV valid or invalid |
| ***Procedure :*** |
| {r} ← #database (cloud server) |
| var i; |
| for i := o to Length({r} -1) |
| If (DIV == {r}[i]) |
| Accept the packets |
| else |
| Reject the packet |
| endif |
| endfor |

If the Value of DIV exists into the range of DIV {r} then accepts the packets or otherwise rejects the packets.

Setp5) Then validate the Message Integrity Code (MIC) with new generated Message Integrity Code (MIC1) using the MICHAEL MIC method with the input of source and destination device MAC address and Paired wise transient key VIdent.

| **Algorithm : Validation of MIC** |
|---|
| ***Input :*** MIC from ciphertext |
| $MAC_{MU}$, $MAC_{CS}$ ,VIdent, plaintext |
| ***Output :*** MIC valid or invalid |
| ***Procedure :*** |
| var I , $MIC_1$ |
| $MAC_{MU}$, $MAC_{CS}$ ,VIdent, plaintext → MICHAEL MIC() |
| MICHAEL MIC() → $MIC_1$ |
| If (MIC == $MIC_1$) |
| Accept the packets |
| else |
| Reject the packet |
| endif |

In the MICHAEL MIC method, all inputted values MACMU, MACCS , VIdent, plaintext are the same as it is like on source device or mobile devices hence its output at cloud server MIC1 must be same as MIC otherwise reject the packets.

Step 6) In the last step on 32-bit plaintext 32-bit CRC-32 error detection algorithm applies. Everyone knows the working concept of CRC-32 error detection. Here we can say that using CRC-32 detects the error in plaintext. If an error exists in plain text then send the negative acknowledgment to the sender and demands retransmission of packets otherwise accept the packet.

Hence by using our proposed theory, we achieve the security algorithm for encrypting the information over mobile cloud computing.

## CONCLUSION

So far each methodology, we have discussed in our thesis paper, mainly based on how to protect information over wireless communication. We have combines various encryption and decryption strategies in our MCC Secure Protocol Layer (MSPL). The MAC address, IMSI, username, and password, encrypting & decrypting keys can be a hack or forged. So in our protocol MSPL various cryptographic features of different algorithms like RC5 algorithm, TKIP, MICHAEL MIC method, and CRC-32 error detection into one cryptographic method and provides the security to information during wireless communication. For encrypting and decrypting information, we totally avoid public key as well as the sharing of keys between different entities of MCC. The major improvements in our proposed MSPL protocol, we use a cryptographic message integrity code (MIC), new DIV sequencing values per packets, key mixing function with secret key calculated by Diffie-Hellman key exchange scheme.

Finally, we can say that using multifactor cryptography for information during transmission, our protocol provides security proof communication over wireless networks. In the next paper, we will discuss the security mechanism for wireless signals in Mobile Cloud Computing.

## REFERENCES

[1] Augmentation Techniques for Mobile Cloud Computing: A Taxonomy, Survey, and Future Directions
BOWEN ZHOU and RAJKUMAR BUYYA, The University of Melbourne, Australia, *ACM Comput. Surv.* 51, 1, Article 13 (January 2018), 38 pages. https://doi.org/10.1145/3152397

[2] Mobile Cloud Computing: A Comparison of Application Models,Dejan Kovachev, Yiwei Cao and Ralf Klamma,Information Systems & Database Technologies,RWTH Aachen University,Ahornstr. 55, 52056 Aachen Germany,fkovachev, cao, klammag@dbis.rwth-aachen.de

[3] Mobile Cloud Computing : Architecture , Algorithms and Application. Debasis De

[4] A Novel Approach for optimal Multimedia Data Distribution in Mobile Cloud Computing. Author : Pham Phuoc Hung,Mohammad Aazam , Tien-Dung Nguyen and Eui-Nam Huh.Department of Computer Engineering, Kyung Hee University, Yongin 446-701 Republic of Korea.Published in : Hindawi Publishing Corporation, Advances in Multimedia , Volume 2014, Article ID 137296. http://dx.doi.org/10.1155/2014/137296

[5] Wikipedia

[6] Resource Allocation and Management Techniques for Network Slicing in WiFi Networks By Matías Richart November 2019 . University of De La Republic

[7] A Security Architecture for 5G Networks, Ghada Arfaoui, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix

Klaedtke, Prajwol Kumar Nakarmi, Mats Näslund, Piers O'Hanlon, Juri Papay, Jani Suomalainen, Mike Surridge, Jean-Philippe Wary, and Alexander Zahariev
Published in Citation information: DOI 10.1109/ACCESS.2018.2827419, IEEE Access
[8] Power Efficiency Analysis of Multimedia,Secured Mobile Applications, Author : 1] Marius Marcu "Politehnica" University of Timisoara,2 V. Parvan Blv. Timisoara, Timis, Romania 0040-256-403263, marius.marcu@ac.upt.ro
[9] Security Protocol for Cloud Based Communication,
R. Suganya1* and S. Sujatha2†
*1Department of Information Technology, Thiagarajar College of Engineering,*
*Madurai India and 2Department of Computer Applications, Anna University, Trichy, India*
*Publisher :* Dinesh Goyal, S. Balamurugan, Sheng-Lung Peng and O.P. Verma (eds.) Design and Analysis of
Security Protocol for Communication, (247–254) © 2020 Scrivener Publishing LLC
[10] A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication
Michael Heigl[1], Martin Schrammy[2] and Dalibor Fiala[1]
[1]University of West Bohemia, Pilsen, Czech Republic Email: fheigl, dalfiag@kiv.zcu.cz
[2]Deggendorf Institute of Technology, Deggendorf, Germany Email: fmichael.heigl, martin.schrammg@th-deg.de
[11] Packet Encryption for Securing Real-Time Mobile Cloud Applications
Ajay D M1 & Umamaheswari E1 School of Computing Science and Engineering, VIT Chennai,
Chennai, India Published : Mobile Networks and Applications (2019) 24:1249–1254
https://doi.org/10.1007/s11036-019-01263-1
[12] Packet-in-Packet: Concatenation with Concurrent Transmission for Data Collection in Low-PowerWireless Sensor Networks
Peilin Zhang,∗ Xiaoyuan Ma,†‡ Oliver Theel∗ and Jianming Wei†
*∗Carl von Ossietzky University of Oldenburg, Germany*
*†Shanghai Advanced Research Institute, Chinese Academy of Sciences, China*
*‡University of Chinese Academy of Sciences, China*
*Email: {peilin.zhang, theel@informatik.uni-oldenburg.de}, {maxy, wjm@sari.ac.cn}*
*Published* 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)
978-1-5386-7308-9/18/$31.00 ©2018 IEEE
DOI 10.1109/ICPADS.2018.00117
[13] Survey of Security Technologies on Wireless Sensor Networks
Qiuwei Yang,1 Xiaogang Zhu,2 Hongjuan Fu,1 and Xiqiang Che3
*1College of Information Science and Engineering, Hunan University, Changsha, China*
*2School of Computer Science and Information Engineering, Hubei University,Wuhan, China*
*3ChangSha LeGou Network Technology Co. Ltd., Changsha, China*
*Published :* Hindawi Publishing Corporation, Journal of Sensors Volume 2015, Article ID 842392, 9 pages
http://dx.doi.org/10.1155/2015/842392
[14] Code-Hopping Based Transmission Scheme for Wireless Physical-Layer Security
Liuguo Yin 1,2 and Wentao Hao2,3
*1Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China*
*2EDA Laboratory, Research Institute of Tsinghua University in Shenzhen, Shenzhen, China*
*3School of Aerospace Engineering, Tsinghua University, Beijing 100084, China*
*Published :* Hindawi. Wireless Communications and Mobile Computing Volume 2018, Article ID 7063758, 12 pages
https://doi.org/10.1155/2018/7063758
[15] End-to-End Efficient Heuristic Algorithm for 5G Network Slicing
Amal Kammoun[1,2], Nabil Tabbane[1], Gladys Diaz[2], Abdulhalim Dandoush[3] and Nadjib Achir[2]
[1]MEDIATRON Laboratory, University of Carthage, Sup_Com, Tunisia
[2] L2TI, Paris 13 University, Sorbonne Paris Cite, France
[3] ESME Sudria, France
{amal.kammoun, nabil.tabbane}@supcom.tn
{gladys.diaz, nadjib.achir}@univ-paris13.fr
abdulhalim.dandoush@inria.fr
Published : 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications 1550-445X/18/$31.00 ©2018 IEEE
DOI 10.1109/AINA.2018.00065