END TO END SECURITY ENHANCEMENT IN SIP USING SSAS FOR AD-HOC NETWORK

K.Shanmugapriya[1] and P.Shanthi Bala[2]

[1,2] Department of Computer Science, Pondicherry University, Puducherry, INDIA.

Abstract

Session Initiation Protocol (SIP) is a signaling protocol which is used in application layer for call initiation and establishment. SIP offers various services viz. video conferencing, instant-messaging and multimedia applications. It has been designed for infrastructure environment which provides no guaranteed connection with server. The deployment of SIP in distributed environment for example Ad-Hoc network has some security issues like end-to-end security, secure Neighbor Discovery (ND), message integrity and privacy related attacks. Thus, the unique authentication is required to overcome these issues. In this work, Simple Secure Addressing Generation Scheme (SSAS) algorithm with social network paradigm is adopted to provide secure communication in less network traffic during registration process, call initiation and termination in Ad-Hoc network. In initial phase of SSAS, authentication is performed for newly joining nodes in the network. Hence, there is a need of an approach to securely exchange the parameters during the authentication phase. In this paper, the approach to securely exchange the parameters through online using Neighbor discovery protocol (NDP) messages have been proposed. It has been implemented using Qualnet simulator. The performance of the proposed approach is evaluated through the performance metrics such as packet dropped ratio, session establishment time, mean end to end delay, average jitter and data transmission. From the results, it has been proved that our proposed approach reached desired security level with high degree of performance in Ad-Hoc network.

Keywords

Session Initiation Protocol (SIP), Ad-Hoc network, SSAS algorithm.

1.Introduction

Ad-Hoc network is an emerging paradigm in telecommunication network. It works with wireless, dynamic infrastructure less architecture. It provides ubiquitous services to users. The combination of the developing technologies like IP Telephony and multimedia services in the Ad Hoc network gives remarkable development in current communication network. In recent years, two protocols such as H.323 and SIP were used by the telecommunication service providers. The protocols address signaling and multimedia service control problems through different approaches. H.323 is an umbrella standard developed by ITU-T in 1996. Initially, H.323 was designed to support multimedia conferencing. It was extended with various versions like H.32x series to enhance the services. The services provided by H.323 are such as multipoint conferencing, call management, accounting, audio and video, security and codecs.

On the other hand, SIP is developed by Multiparty Multimedia Session Control (MMSC) working group of the IETF in 1998. It is an upper level protocol i.e. application layer level which is used to establish two-way communication session. Even though, SIP is not more prominent than H.323, it can be used to adapt new features and modifies the program easily. It was originally

developed for multimedia conferencing. Generally, in public access network like Internet, everyone can access and sent packets. The security issues like eavesdropping, packet capturing, and interception of network traffic signals can be achieved without any technical difficulties. The attacks can be pointed out in both hardware and software components. In terms of software, lots of monitoring tools are available like Wireshark [29], Aircracking [24], iStumbler [25], MacStumbler [28], KISMAC [26], KISMET [27] can be used for interception in network traffic. Many application programming interfaces are accessed to attack the network signaling systems. For secure communication, advance security mechanisms are needed to safeguard the sessions. Simple Secure Addressing Generation Scheme (SSAS) is used with social paradigm to mitigate the issues that arises during session establishment. SSAS algorithm generates randomized Interface Identifier (IID) in IPv6 address when the nodes are joining in the network. It also generate signature for ensuring secure Neighbor Discovery and message integrity. To ensure the authenticated node, the randomized IPv6 address is used as a certificate for accessing new network. This method is deployed in the SIP along with social network pattern for achieving secure communication in Ad-Hoc environment.

Section 2 discusses about the existing work with available security mechanisms. Section 3 delivers the background work about SSAS algorithm. Section 4 explains technical issues which were not addressed in previous research work. Section 5 discusses SSAS Scheme with Social Paradigm. The implementation and analysis of the proposed approach is described in Section 6.In Section 7 references are provided and finally Section 8 concludes the paper.

2. Related Work

The framework for Ad-Hoc network in SIP was proposed by Hechmi Khlifi et al[10]. It discussed about discovery, establishment and end of the SIP sessions. The improvisations were established on network layer routing protocol, SIP REGISTER methods in application layer and achieved scalability by clustering approach.

Distributed SIP was implemented in Ad-Hoc network. This framework was presented by Leggio et al [11]. SIP REGISTER message was broadcasted to neighboring nodes and the binding information was attached with this message. The binding information was stored in local cache for proxy server to lookup process during INVITE message. Similar type of message for binding information is sent to users. It includes two types of messages such as SIPRREQ and SIPRREP. This method was proposed by Nilanjan Banerjee et al[4]. A control message is in the form of AODV RREQ and RREP messages.

“Hello” message is broadcasted to neighbors for updating the presence of SIP client. This approach is framed by O'Doherty[14]. SIP gateway was introduced to communicate between SIP clients in Ad-Hoc network to the Internet user’s. The register and proxy server is available in gateway which includes additional header fields such as “Path” and “Record-Route”. Balov et al [3]proposed the similar gateway concept along with advertising by using routing messages. Unique address is attached as prefix and broadcast to every nodes. The gateway confirmation messages were unicasted to gateway which contains the global address of MANET nodes.

Mutual authentication in SIP was proposed by Yaghoobian et al[18]. End to end security can be achieved among users and operators by using multi-crossed authentication techniques. To avoid overlapping of multi-operators, Subscriber Identity Module (SIM) based authentication was carried out.

Ono et al[15] proposed a mutual authentication with extension of firewall configuration to filter out signals by port number. Overhead of firewall configuration was moved to token mechanism to reduce the security problems. SIP security problems were analyzed in Geneiatakis et al[7] and discussed about the issues. The protection of SIP signaling is extremely difficult than PSTN which is due to lack of control points in SIP. The extension has been made with additional capability which helps to design and develop secure SIP services in order to provide secure services. Secure authentication mechanism for SIP was proposed by Yang et al [20] and it uses Diffie-Hellman key exchange algorithm for secure sharing of key. It is very difficult for attackers since it is based on discrete logarithm. This scheme comes with high computational cost.

New authentication scheme for SIP was proposed by Durlanik et al[6] using Elliptic Curve Diffe-Hellman (ECDH) algorithm. It is very difficult for the attacker to compromise because it was designed based on discrete logarithmic algorithm and the key size is small with low computation cost and also reached desired level of security.

HTTP digest authentication using ECC was introduced to overcome the issues in Durlanik's and Wu's schemes. It mitigated password guessing attacks, Stolen-verifier attack etc. which was proposed by Yoon et al.[21].

Secure authentication and key agreement mechanism (SAKA) was framed by Wang and Zhang [21]. This mechanism gives certificate through Trusted Third Party (TTP). It generates private key and HTTP authentication (handshake process) for key agreement mechanism.

Liao and Wang[23] improved a method proposed by Wang and Zhang [21] with self-certificate public key based on Elliptic Curve Cryptography (ECC) while keeping the main structure of HTTP digest authentication. This scheme also uses TTP for generating private key for users.
Ring et al.[18] proposed a method called Identity based cryptography for SIP authentication. The public key act as a user's function, the private key is generated by Trusted Authority (TA). It follows the structure of HTTP digest authentication, but uses ECC based identity which is used to generate secure session key between two participants. The computation cost is high due to the use of elliptic pairs of keys. It is suitable only for constrained devices such as PC, PDA, and Smart Card etc.

A Cryptographically Generated Address (CGA) [1] is self-certified IPV6 address which binds a public key with IPV6 address of the public key owner. Its mechanism is to compute cryptographic one way hash function of the public key and auxiliary parameters.

Peterson et al[16] framed a method to enhance authentication for SIP and proposed in IETF. It has two header fields namely identity and identity-info. SIP User agents connect and authenticate with SIP server. Subsequently, it signs the message after the message has been received from the User Agent (UA) with the use of its domain certificate. The digital signature is included in the identity header field and URL of the web server is included in identity-info header field.

Geneiatakis and Lambrinoudakis[7] introduced new SIP extension called "Integrity-Auth". This work concentrates on SIP signaling Attacks, message integrity and authenticity. The value of new header field acts as a hash value of user's password and combined with some unknown parameters. The verification of new header value provides the message integrity and authenticity of user.

Stuedi et al[30] use a local cache to store users binding information. They propose a middleware infrastructure for session setup and management in MANET called SIPHoc. They use SLP for SIP endpoints discover. One of the SIPHoc components is MANET SLP, which provides fully distributed registration and lookup services. An SLP service query is sent via routing messages by piggybacking the binding information onto these routing messages. This is done through a routing handler plug-in. The routing handler is a software module that receives raw routing packets and generates alternate packets which includes the binding information. The router handler makes SIPHoc independent of any routing protocol. Also, each node has a SIPHoc proxy that serves as an outbound SIP Proxy for the local SIP application. Other components of SIPHoc include gateway and connection providers. While the gateway provider turns a node into a gateway, the connection provider manages the node's connection to the internet.

Rafiee et al [17] proposed randomized IID (Interface Identifier) in IPv6 network using SSAS algorithm. In this, unique address is generated for newly joining network with reduced time and higher security level. This mechanism can be implemented in limited resource and are available for computation like Ad-Hoc network, Sensor network etc.

In Ad-Hoc environment, a precise security measure is needed for mitigating all these issues. So, the randomized security parameters are required to authenticate the newly joining nodes into the network with less time consumption.

3. Background

Before sending SIP message in Ad-Hoc environment, precise technique is used to generate randomized Global IP address for joining into new network with secure certificate and signature. This will be achieved by using Simple Secure Addressing Generation Scheme (SSAS) algorithm.

3.1 SSAS Generation process

SSAS algorithm is examined in the IPv6 based network[17]. It generates randomized IID to secure communications in Ad-Hoc network. This process consists of four modules to reach desired level of security as follows:

1. Generation of SSAS address.
2. Signature Generation.
3. Generation of NDP message.
4. SSAS Verification process.

i. Generation of SSAS address :

In initial stage, node can generate its randomized address using SSAS algorithm illustrated in algorithm 1. In this module, a random 16 byte modifier, 1024 size bits of RSA key pair (public/private key) with 2 days validation period, time stamp to avoid network delay has been used. The generated address is attached in SSAS signature as Global IP address shown in figure 1.

Time Stamp (8 Bytes)	Public key (16 Bytes)	Global IP address (16 Bytes)	Other Option (Variable)

Figure 1. SSAS Signature

Algorithm.1: SSAS Address Generation

```
1:  Input :Modifier(16 byte) as M, RSA Key Pairs(1024 bits) as K,
    Time Stamp(8 byte) as T, Public Key as PK, Start Index for SHA2 array as SI
2:  CONCATE  x=(M,PK,T)
3:  DIGEST x2= SHA2(x)
4:  GENERATE  SI
5:  if SI <= 20   then
6:       CONCATE  x3=(SI, x2)
7:  else
8:       GENERATE new SI
9:  end if
10: GENERATE  x4= 32 Leftmost bits(x3)
11: SET 'u' bit AND 'g' bit as 1 in x4
12: WRITE  x4                        // Partial Interface ID(32 bits)
13: SET  x5=2nd Byte(x4)             // x5 is Start Field Index
14: if  x5<= SIZE(PK)  then
15:    x6= x5-4 (Bytes)
16:    WRITE  x6                     // x6 is Start field index
17: else
18:   x6= x6 >> 2
19:  WRITE x6
20: end if
21: CONCATE  PK1=(x6,PK)  // Start Field Index and Public key
22: CONCATE  y=(x4,PK1 )    // x4(32 bits),pk1(32 bits)
23: CONCATE  IP=(SN, y)      // SN is Subnet (64 bits) , z is Interface ID(64 bits)
24: if  IP == Global Address List  then
25:    INCREMENT m BY 1
26:    BEGIN from x
27: else
28:    WRITE  IP                  // IP as SSAS Address
29: end if
```

ii. Signature Generation:

Digital signature is generated to prevent from IP spoofing attack. This signature is attached with NDP and SIP messages for ensuring the endpoints. The following algorithm 2 generates the digital signature to be attached in NDP message.

Algorithm 2: SSAS Signature Generation

```
1:  Input: Time stamp as T, Received Public Key as PK1,Private Key as PR
    Global IP address as IP, Hash Value of SIP message as HSIP
2:  CONCATE  Plain=(T,PK1,IP,HSIP)
3:  Sign=ENCRYPT(Plain,PR)  // PR is Private Key
4:  WRITE  Sign
```

3.2 SSAS signature data field

SSAS signature data field is included to the NDP messages to verify the sender. When a node receives the Neighboring Advertisement (NA) message in response to its Neighbor Solicitation (NS) message, it shows that the newly joining node claims to its own network address. After SSAS verification, this node modifier is incremented by 1. For second time, same claim message to own the same address, then it is considered as an attack and discard this message.

The following parameters are used as fields in NDP message format.

a. Type: This option should be set to 12.
b. Length: The length of the Signature Data field, including Type, Length, Signature, Reserved, pub key Len, public key and padding must be multiples of eight.
c. Reserved: A 2 byte field reserved for upcoming progress. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.
d. Other Len: The length of other options in multiples of eight. The length of this field is 1 byte.
e. Subnet Prefix: This is the router subnet prefix.
f. Pub Key Len. The length of the public key in multiples of eight.
g. Public key. Base64 format of the public key.

3.2.1 Generation of NDP message

Once the Global IP address is generated, the DAD process is performed by sending Neighbor Solicitation (NS) message to avoid collision in the network. SSAS signature is added into the ICMPV6 format of NS message. Time stamp is also included in NS message. Figure 2 shows the NDP message format with its parameters.

<table>
<tr><td>IPV6 Header</td><td>ICMPV6 Header</td><td colspan="2">ND message Specific data Next Header=58</td></tr>
<tr><td>Type =13
(1 Byte)</td><td>Length
(1 Byte)</td><td colspan="2">Reserved
(6 Byte)</td></tr>
<tr><td colspan="4">Time Stamp</td></tr>
<tr><td>Type = 12
(1 Byte)</td><td>Length
(1 Byte)</td><td>Reserved
(2 Byte)</td><td>Other Length
(1 Byte)</td></tr>
<tr><td>Subnet Prefix
(8 Byte)</td><td>Pubkey Len
(1 Byte)</td><td colspan="2">Public Key in base64 format</td></tr>
<tr><td colspan="4">Other Options</td></tr>
<tr><td colspan="4">SSAS Signature</td></tr>
<tr><td colspan="4">Padding</td></tr>
</table>

Figure 2. NDP message format [17]

3.2.2 SSAS Verification process

Verification part is implemented after the NDP message received by the receiver. The following algorithm 3 is used for verification process for ensuring legitimate node.

Algorithm 3: SSAS Verifications process

```
1:  Input: NDP message and SSAS Signature, Time Stamp asT1,T2,
    Public Key as PK, Start field index as x5, Received Interface IID as ry,
    Subnet prefix as SN, Received Hash value of SIP message as rHSIP.
2:  GET  T1                                  // Obtain from NDP message
3:  GET  T2                                  // Obtain from user's node
4:  if (T2-600)<= T1 <= (T2 + 600) then      // Checks for network delay, SET as 10 min
5:  if (PK!= rPK) then                       // rPK is receiver's Public Key list
6:  if  x5<= SIZE(PK)  then
7:          x6= x5- 4 (in Bytes)
8:          WRITE  x6                        //Start Field Index
9:  else
10:         x6= x6 >> 2
11:         WRITE x6
12: end if
13: CONCATE  rPK1 =(x6,PK)
14: For i=1 to 32 bits do
15:     WRITE rPK2 = rPK1 [i]                // 32 Leftmost bits, including x6.
16: end for
17: for i=64 to 32 bits do
18:     WRITE ry2 = ry[i]                    // 32 Rightmost bits of IID
19: end for
20: if rPK2 == ry2 then
21:     GET SN
22: else
23:     WRITE Discard Message
24: end if
25: CONCATE rPlain = (T1,PK,SN,ry,rHSIP)
26: GET rSign                                // Obtain rSign from SSAS Signature data field
27: rSign = DECRYPT(Plain,Rpk)
28: if Sign== rSign then
29: if rPlain=Plain then
30:     BEGIN process
31: else
32:     WRITE Discard Message
33: end if
34: else
35:     WRITE Discard Message
36: end if
37: else
38:     WRITE Discard Message
39: end if
40: else
41:     WRITE Discard Message
42: end if
```

The reverse process is carried out along with the comparison of security parameters in the friend's list. If the parameters get matched then he/she will be treated as authenticated user.

4. Technical Issues In SIP

SIP message contains various fields like source address, destination address, and security parameters. The content of the message is represented in text format. It can be spoofed or modified by the attacker. Trust association between the nodes in Ad-Hoc network leads to privacy related attacks. In addition, the attacker can spoof the legitimate user's identity and IP address ownership. Some of the following listed issues have not been focused in various research works**.**

Issue 1: If user wants to deploy SIP protocol to support an open access, additional security features are needed to trust the anonymous users. There is a possibility of vulnerability attack during the security parameter exchange through off-line mode.

Issue 2: Even digest authentication, the attacker can trace the contact field in the SIP message and change the IP address of the user. Even, the attacker can identify the security parameters by comparing the results using some digest algorithm. This can be achieved by brute-force search.

Issue 3: Attacker can spoof the user's identity and modify the SIP REGISTER message to expire the Header field into zero. This leads to shut down the devices and no more calls can be sent. This issue is not tackled well in available standards.

Issue 4: The "Contact header field" can be modified by hacker which leads to IP Spoofing attack and results in Denial of Services. This attack redirects the caller to the attacker's device.

Issue 5: SIP messages can be modified after the spoofing of user's identity. This leads to send SIP BYE, CANCEL messages to the caller which results in call tear down attack.

Issue 6: Message Integrity is needed to verify the content of the message. The modification through impersonation causes integrity issue.

Issue 7: In IPv6 address based network, randomized IID was needed to protect the privacy of the user's node. This can be achieved by two mechanisms viz. CGA [1] and privacy extension[12]. It generates the address and security parameters which can be exchanged in offline mode. This process leads to offline attacks and IP spoofing attack.

During the generation process, CGA [1] takes more computational time when 'Sec' value is higher. The verification process in receiver's side, inverse steps is needed to evaluate the IP address Ownership, takes additional time for Verification. Privacy Extension [12]provides a partial protection to the privacy issues. It cannot prevent IP address ownership, IP spoofing attacks.

In order to palliate these issues, strong security mechanisms are needed to ensure secure communication in SIP in Ad Hoc network.

5. Proposed Work

In order to overcome these technical issues, an efficient mechanism is required for Ad-Hoc networks. The proposed mechanism is a Simple Secure Address Generation Scheme (SSAS) algorithm, along with SSAS Signature is provided to protect the system from the issues discussed in the previous section. The deployment of the proposed algorithm in the decentralized environment, a desired level of security is essential for the node which has limited resources with reduced computational time. To achieve this, SSAS scheme is deployed in the IPv6 based network. The IPv6 address which contains two parts such as Subnet prefix (64 leftmost bits) which is used to locate the user's location and Interface ID (64 rightmost bits) which is interface ID of the particular node. IID is able to modify by any required randomized mechanisms.

For secure communication in SIP, various security mechanisms are proposed. The existing systems are cracked by the attackers, the unique authentication or security methods are required for ensuring confidentiality, privacy, authentication and message integrity.
In proposed work, the authentication task is distributed in SIP architecture with combination of SSAS scheme and Social Network Paradigm which is deployed in IPv6 based network. Assume that every node has capability to generate SSAS address with the digital signature using SSAS algorithm. In addition, authenticate callee using identity management in SIP. The SSAS address is combined with social network paradigm which provides authentication and helps to prevent from various attacks like IP Spoofing, Impersonation attack, message attacks, etc.

At first, each node generates randomized IID with Subnet prefix which is combined to form a SSAS address using SSAS algorithm in IPv6 format. This address is attached in the NDP message for secure ND. SSAS address generation algorithm is discussed in section 3.1.SSAS address is generated by using public key along with security parameters of an address of the owner. It generates self-certificate and digital signature without rely on centralized certificate authority. It also attaches the digital signature with message for validation of IP address ownership. SSAS verification method which is discussed in Section 3.3 is used to validate the user's identity from initial phase onwards, while NDP message is send to the new joining network. For security purpose, the time period of Owner's public key is valid for 2 days only. Thus, the same certificate cannot be used for every new joining network.

Once authentication process completed, the receiver stores the sender's SSAS address and SSAS security parameters in his/her friend list. An extension specification is utilized from Identity management of SIP for authentication [16]. Additionally, two new header fields are added to SIP messages such as "Identity" field which holds the digital signature of the SIP message and "Identity-Info "field which holds the SSAS address of address owner. It involves in two phases to provide security to SIP message.

The first phase discusses about the secured SIP message generation with its merits in sender's side as follows (Figure 3):

1. After the authentication succeeds, the original SIP message is hashed by SHA2 mechanism.
2. Time Stamp of the sender, Sender's public key, Global IP address (using SSAS algorithm) and hash value of SIP message is encrypted using sender's private key to form SSAS digital signature which is included in Identity header field.
3. As discussed before, SSAS address is generated using SSAS algorithm is included in Identity-Info header field.

4. Finally, secured SIP message is generated, and then it is forwarded to destination node. This format is consequently applied for every SIP messages to prevent from privacy based attacks and spoofing attacks like IP spoofing, spoofing of address ownership.

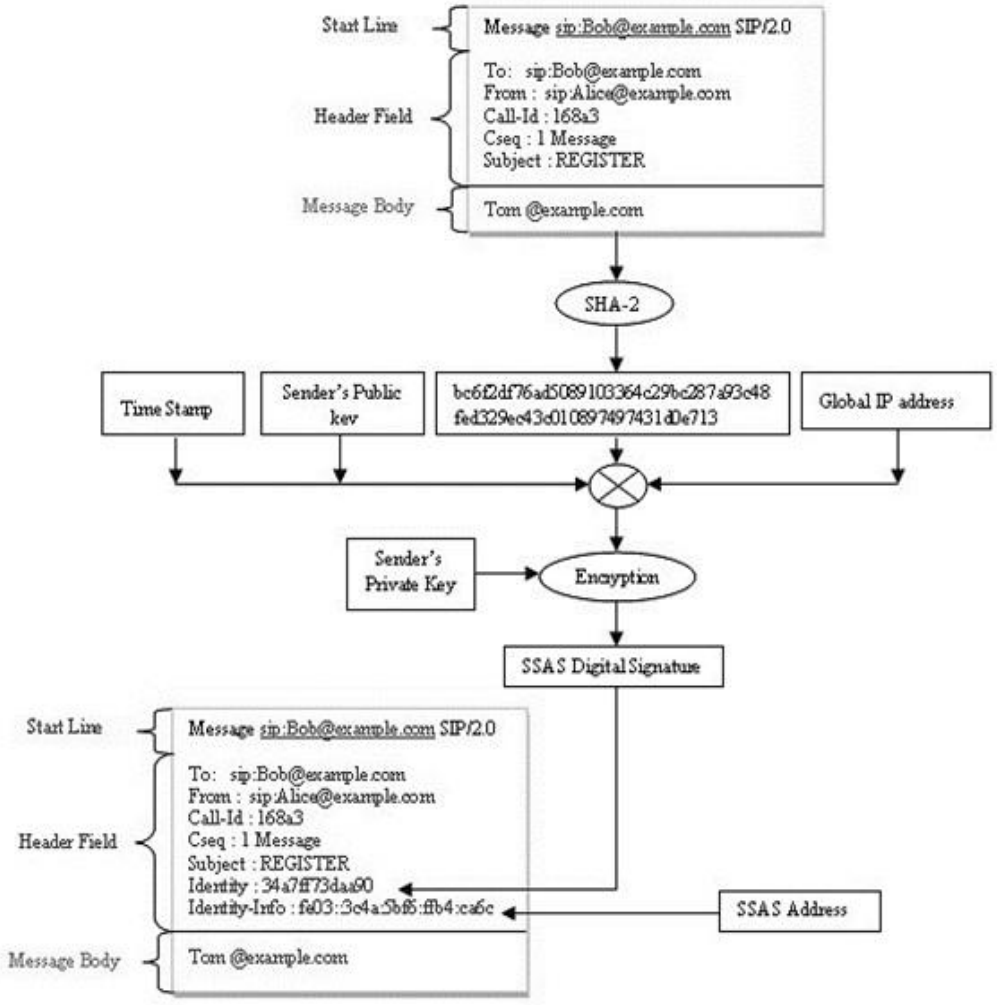

Figure 3. A Secured SIP message generation process

In second phase, verification of SIP messages can be performed by invoking SSAS signature and using SSAS signature. Verification is accomplished by ensuring the SSAS address of the message originator and identified the security parameters from the corresponding user's friend's list to guarantee the message integrity as shown in figure 4.

1. A node sends SIP REGISTER message to another node, it checks SSAS address for his/her friend list, instead of identity based negotiation.
2. The SSAS digital signature is decrypted using sender's public key from friend's list, it forms plain text. The plain text consists of time stamp, Global IP address, hash value of SIP message and sender's public key. The received plain text has been validated with SSAS parameters in his/her friend's list to ensure the address ownership with message integrity.

3. At last, verification succeeds, if both the processes match. Then the receiver establishes the call for communication otherwise call will be discarded. If non-friend is sending SIP message, again it checks in the friend's list. If callee's identity parameters are not present, it sends Lookup messages to his/her friends. Any of his/her friends authenticate the identity of non-friend; node can store and accept the non-friends call for future communications. The proposed authentication mechanism prevents from attacks and ensures the privacy of user's identity with reduced computation time.

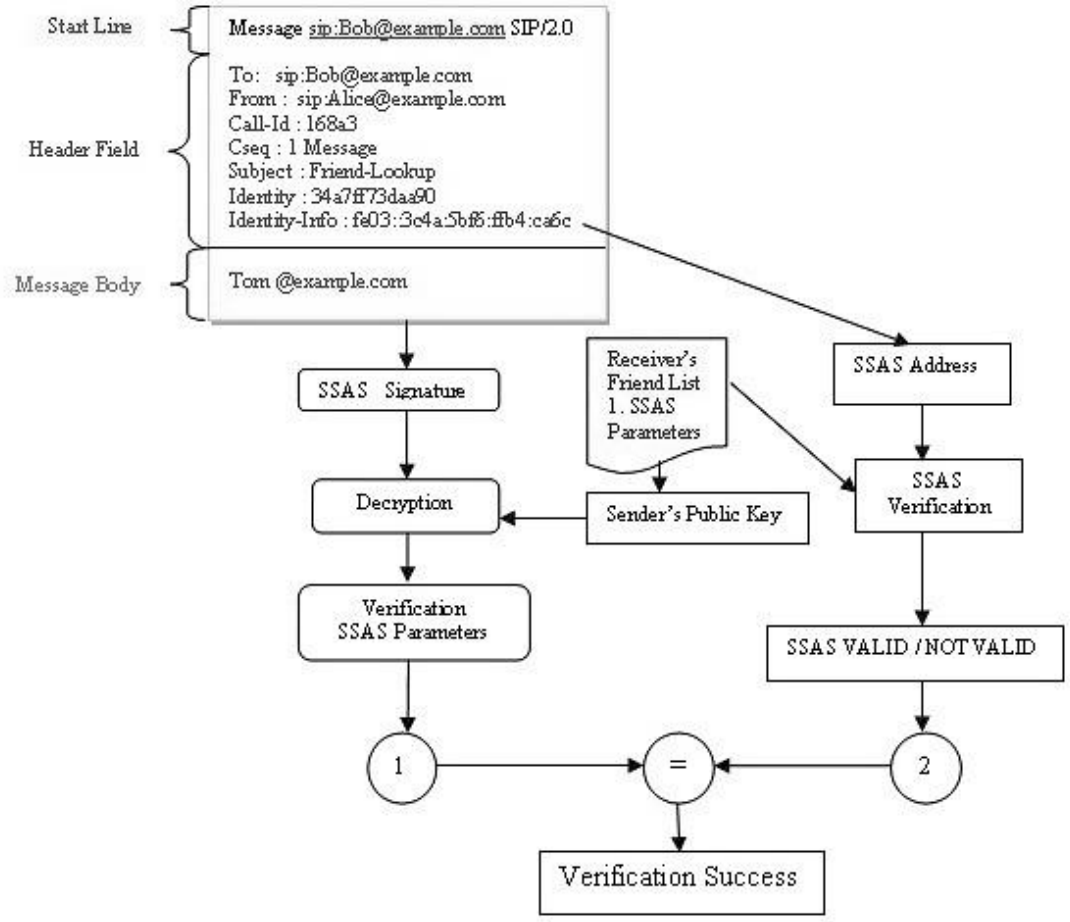

Figure 4.Verification of SIP message

6. Evaluation And Implementation

The proposed system is implemented in Qualnet simulator in windows environment. The new extension is implemented in SIP protocol to achieve the security level. In this scenario, 8 nodes are considered for simulation. Due to small space of deployment, the nodes can be placed randomly within 500x500 areas. Every node is configured as SIP enabled node with security parameters (Security Enabled). The session initiated time at 60s and session ended time at 240s. So, the total session time is 180s. In this environment eight numbers of nodes are used in for simulation, among eight nodes, randomly three nodes are chosen as eavesdropper to enable miscellaneous action in the network. The same setup is designed without security (Security

Disabled) features for comparison. The results are compared with various performance metrics and evaluated.

In order to evaluate, the performance metrics such as packet dropped ratio, session establishment time, Mean end to end delay, Average Jitter and Data transmission are considered and compared with and without security features.

6.1 Packet Dropped Ratio

Packet dropped defines the packet loss due to fluctuation to one or more packets are failed to reach the destination. Figure 5 shows packet dropped level for two scenarios as follows:

i) Inclusive of security parameters named as Security Enabled.
ii) Excluded Security parameters named as Security Disabled.

In this case, our proposed work reduces the packet loss with desired level of security as mentioned in Table 1.

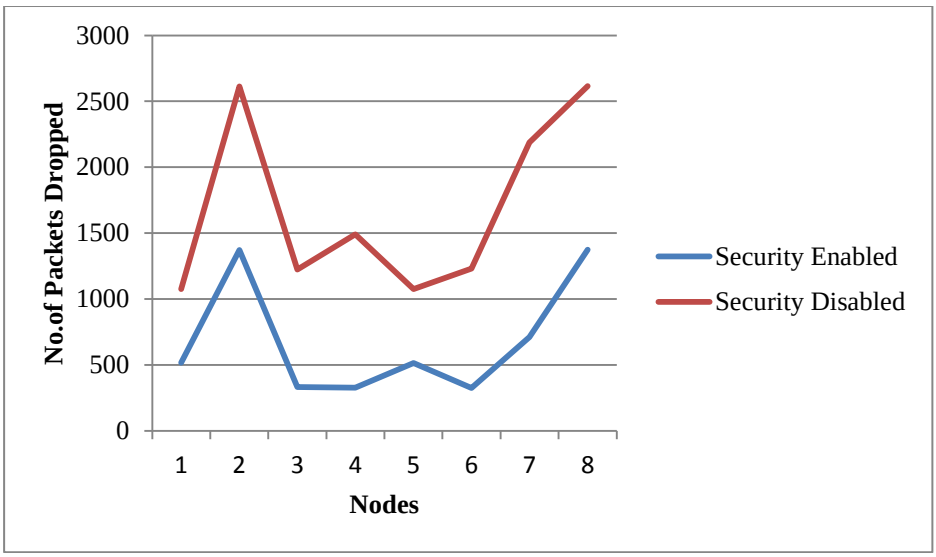

Figure 5. Packet Dropped rates

Table 1. Packet Dropped Rates

Nodes	Security Enabled	Security Disabled
1	516	1076
2	1372	2614
3	333	1224
4	328	1491
5	514	1075
6	325	1230
7	711	2187
8	1374	2615

6.2 Session Established Time

The time taken to establish the media stream for communication is called session establishment time. In our proposed work session establishment time is high due to exchange of security signals as shown in Figure 6.In this scenario, any node can act as eavesdropper and here node 5 is considered as an eavesdropper. So, it doesn't establish the session which is represented in Table 2.

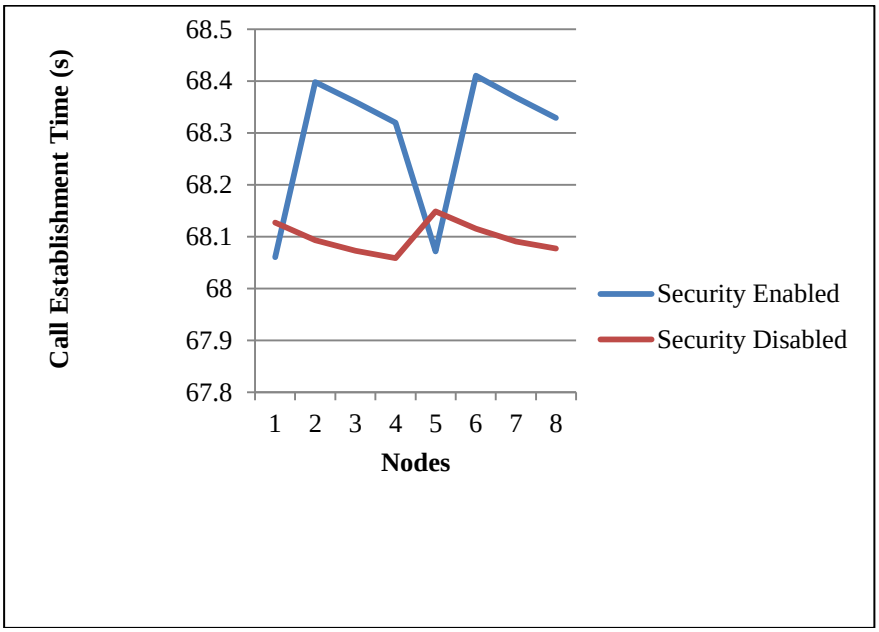

Figure 6. Session Establishment Time

Table 2. Session Establishment Time

Nodes	Security Enabled	Security Disabled
1	68.0607	68.127
2	68.3979	68.0931
3	68.36	68.073
4	68.32	68.0584
5	68.0718	68.1486
6	68.4106	68.1156
7	68.3686	68.0907
8	68.329	68.0769

6.3 Mean end-to-end delay

End to end delay is defined as time taken for packet to reach from source to destination. Delay can be occurred due to high security computation for mitigating attacks. In our proposed work, end to end delay is increased when compared to the disabled security parameter's experiment as shown in Figure 7. The experimental results are shown in Table 3.

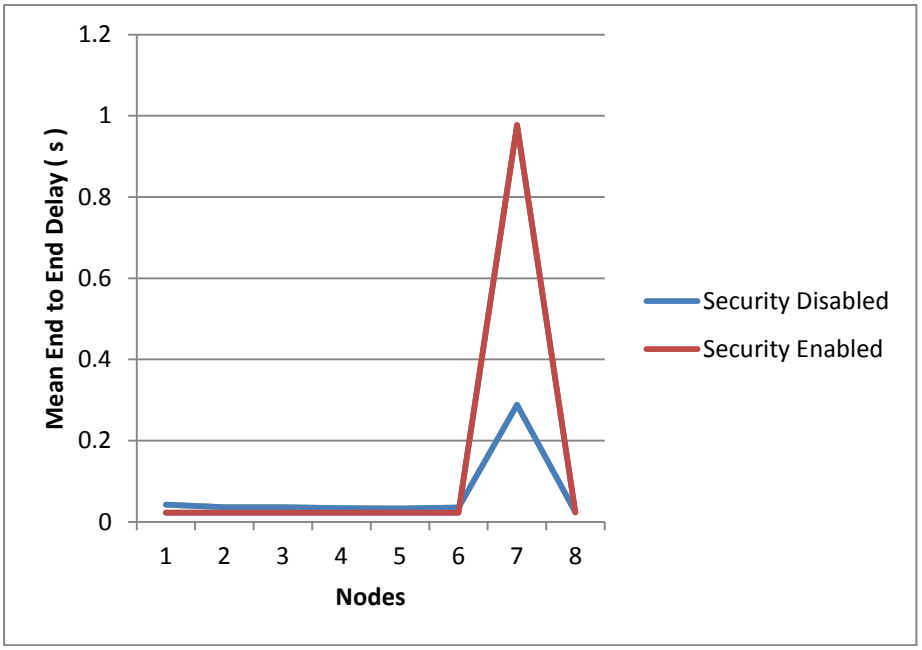

Figure 7. Mean End to end delay

Table 3. Mean End to End Delay

Nodes	Security Enabled	Security Disabled
1	0.042242	0.022718
2	0.035573	0.022783
3	0.03582	0.022522
4	0.033609	0.022602
5	0.032368	0.022569
6	0.035063	0.022556
7	0.977423	0.288015
8	0.02441	0.022998

6.4 Average Jitter

The jitter defines fluctuation of end to end delay from packet arrives. Figure 8 shows security enabled level is high when compared to security disabled one. In Table 4, Average jitter is ranges from 5 – 15ms and 1 – 3 ms for security enabled and disabled features respectively.

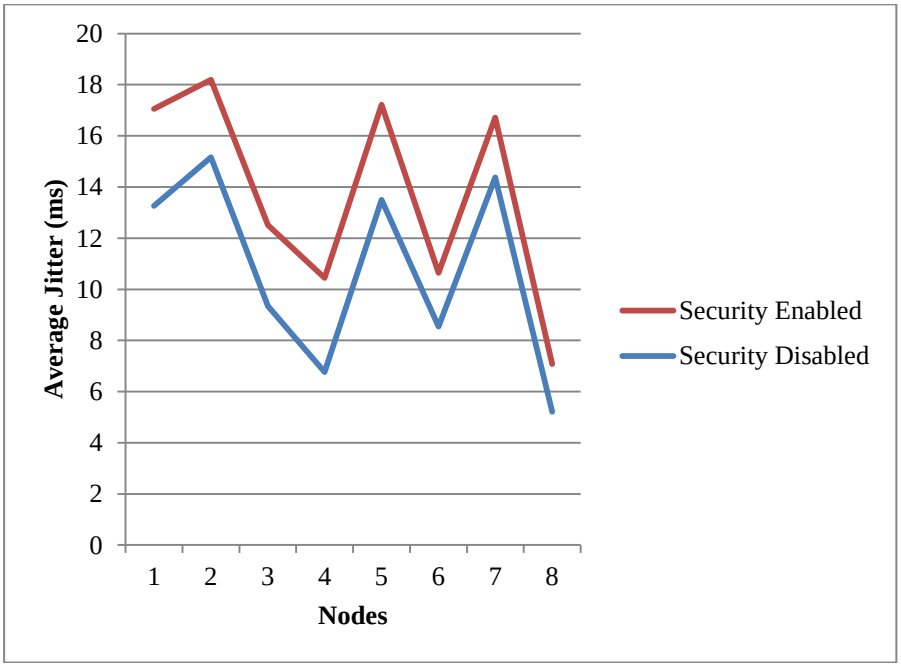

Figure 8. Average Jitter

Table 4. Average Jitter

Nodes	Security Enabled	Security Disabled
1	13.259	3.797
2	15.162	3.033
3	9.341	3.17
4	6.771	3.677
5	13.497	3.715
6	8.54	2.11
7	14.379	2.341
8	5.212	1.864

6.5 Data Transmission

The rate of bits transferred from source to destination across the network. Figure 9show that data transmission rate is increased when the proposed method is applied. The messages are exchanged with high level security measures before communication established. Table 5, shows the data transmission rate comparison result by enabled and disabled security features.

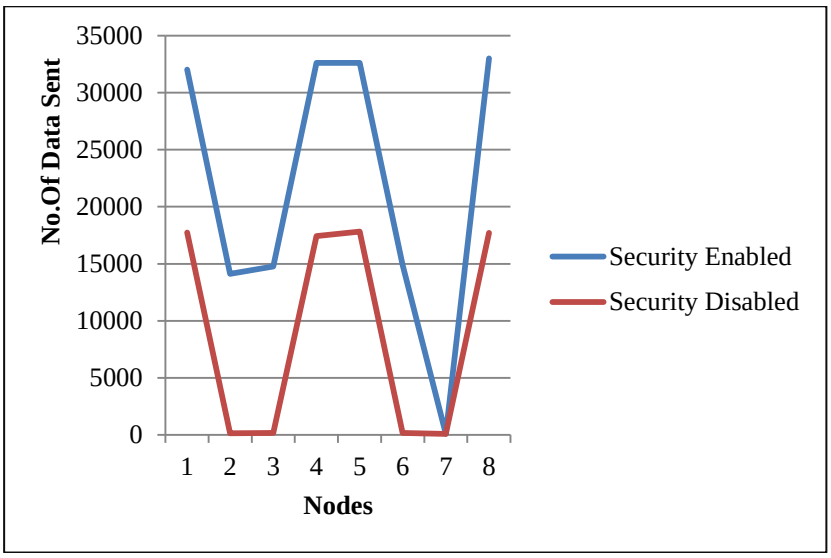

Figure 9. Data Transmission Rate

Table 5. Data Transmission rate

Nodes	Security Enabled	Security Disabled
1	32014	17751
2	14135	157
3	14766	172
4	32598	17420
5	32620	17825
6	14913	184
7	107	109
8	32994	17699

6.6 Comparison results of Average signature generation and verification

The time required for generating the key pairs with different key size usage is shown in the Table 6.This key generation and verification process has done with 8 samples. As a result, the time taken to generate and verify the key pairs takes bearable amount of time in the network environment.

Table 6. Comparison results Average Key generation and Verification using 8 samples.

Algorithm type	Key size	Average Key Generation (microseconds)	Average Signature Generation (microseconds)	Average Signature Verification (microseconds)
RSA	1024 bits	175184	25449	3740
RSA	1280 bits	452802	58080	9544

From the results obtained, it has been proved that the given SSAS algorithm deployed in SIP gives desired level of security measures with increased performance. Highly secure ad hoc environment is developed to monitor the newly joining node with reduced computation time which is suitable for limited resource devices.

7. Implementation

The proposed system is implemented in Qualnet simulation under windows. The new extension is implemented in SIP protocol to achieve the security level. In this scenario, wireless subnet properties are enabled and 14 nodes are considered for simulation. Due to small space application, nodes can be placed randomly within 500 x 500 area. Every node is configured as SIP enabled node with security parameters. The session initiated time is at 60s and session ended time at 240s. So the total session time is 180s. In 14 nodes, 3 nodes are chosen as eavesdropper to enable miscellaneous action in the network. Out of 14 nodes 8 nodes are chosen for end to end communication. The same setup is designed without security features for comparison. Simulation environment is shown in Figure 5.1.

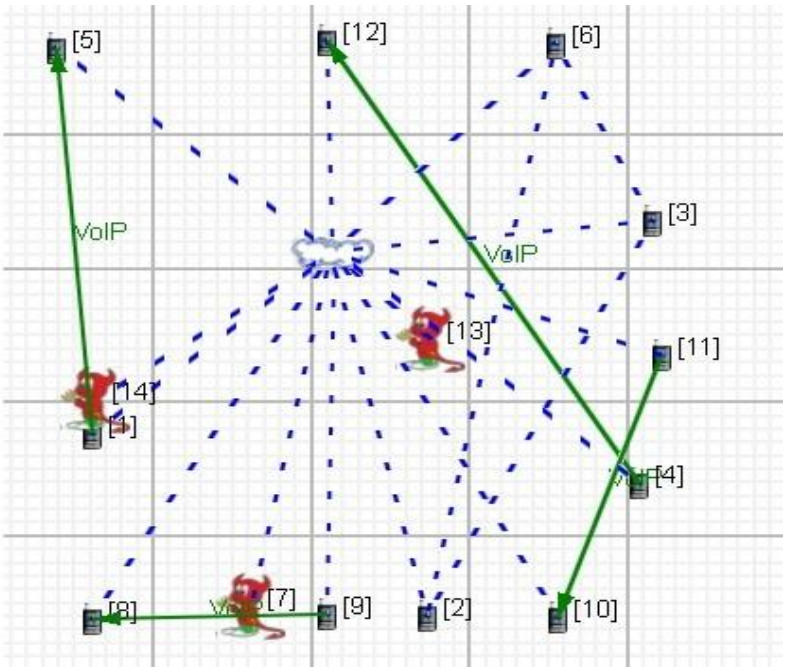

Figure 10. Snapshot of network in Qualnet Simulation

In the above environment nodes 7, 13 and 14 are eavesdroppers, VOIP application established between 1-5, 9-8, 11-10 and 4-12 nodes for communication. The results are compared with performance metrics and evaluated using Graphs (1 - 6). Metrics which has been taken for evaluation are packet dropped ratio, session establishment time, Mean end to end delay, Average Jitter and Data transmission are compared with and without security features environment. Corresponding readings are tabulated in Tables (1- 6) respectively.

References

[1] T. Aura,(2005)" Cryptographically generated addresses (CGA)", IETF RFC 3972. http://www.ietf.org/rfc/rfc3972.txt

[2] J.Arkko, J.Kempf, B.Zill, and P.Nikander, (2005)"SEcure Neighbor Discovery (SEND)", RFC 3971.

[3] K. Balov, K. Kawagoe, and T. Nishimura. (2009)" SIP deployment in integrated mobile AdHoc networks: Centralized and quasi-decentralized approaches". In 11th International Conference on Advanced Communication Technology/ICACT 2009,ISBN 978-89-5519-139-4.

[4] N.Banerjee, Arup Acharya, and SajalDas.(2007)"Enabling SIP-based sessions in Ad Hoc networks",Wireless Networks, ACM ,Vol 13 Issue 4, pp.461 – 479.

[5] T.Cheneau , Andrei Vlad Sambra, Maryline Laurent A,(2011)" Trustful Authentication and Key Exchange Scheme (TAKES) for Ad Hoc Networks,IEEEConference,Network and System Security (NSS)", 2011 5th International Conference on, ISBN -978-1-4577-0458-1, pp.249 - 253.

[6] A.Durlanik and I.Sogukinar, (2005)"SIP authentication scheme using ECDH",World Academy of Science, Engineering and Technology. Available on://http://www.cs.nccu.edu.tw/~d10003/ref1.pdf

[7] D.Geneiatakis and Costas Lambrinoudakis, (2007)"A lightweight protection mechanism against signaling attacks in a SIP-based VoIPenvironment",SpringerLink,TelecommunicationSystems, Vol 36, Issue 4, pp 153-159.

[8] D.Geneiatakis, G.Kambourakis, T.Dagiuklas, Costas Lambrinoudakis and StefanosGritzalis, (2004) "SIP Security Mechanisms: A state-of-the-art review",EURASIP Journal on wireless Communications and Networking, ,Vol 26, pp 184-197.

[9] Mrs. Hemalatha Jai Kumari1 , Dr. A. Kannammal2, (2012)"A Hybrid Certificate Management for Mosbile ad-hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.6.

[10] H.Khlifi, Anjali Agarwal, Jean-Charles Gregoire, (2003)" A FRAMEWORK TO USE SIP IN AD-HOC NETWORKS", IEEE conf ,Electrical and Computer Engineering, IEEE CCECE 2003,Vol.2,ISSN : 0840-7789, ISBN:0-7803-7781-8, pp. 985 – 988.

[11] S.Leggio, J.Manner, A.Hulkkonen, K.Raatikainen,Session, (2005)"Initiation Protocol Deployment in Ad-Hoc Networks: a Decentralized Approach",In 2nd International Workshop on Wireless Ad-hoc Networks (IWWAN).

[12] J. Manner, S. Leggio, and K. Raatikainen, (2006)" An internet SIP gateway for ad-hoc networks",In 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, SECON '06,Vol 3, pp.740-745. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4068362&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4068362.

[13] T.Narten, R.Draves, S. Krishnan, (2007)"Privacy Extensions for Stateless Address AutoConfiguration in IPv6", RFC 4941.

[14] M.O'Doherty. (2001)"Pico SIP", Available on : "http://tools.ietf.org/id/draft-odoherty-pico-sip-00.txt"

[15] K.Ono, S.Tachimoto, and S.Sakaya,(2004)"Security in End-to-end Communications".

[16] J. Peterson and C. Jennings, (2006)"Enhancements for authenticated identity management in the session initiation protocol (SIP)", RFC 4474. https://tools.ietf.org/html/rfc4474

[17] H. Rafiee, C. Meinel,(2013)"A Simple Secure Addressing Generation Scheme for IPv6 AutoConfiguration (SSAS)",IETF RFC 3971.

[18] J.Ring, Kim kwang Raymond, Choo Ernest Foo, and Mark Looi ,(2006)" A new authentication mechanism and key agreement protocol for SIP using identity-based cryptography". http://eprints.qut.edu.au/4422/1/4422_1.pdf

[19] A.Yaghoobian, M.Laurent, KouroshTeimoorzadeh, Jean-Philippe Wary,(2011)"End-To-End Security Establishment Through Operators: SIP Experiment".

[20] Chou-chen Yang, Ren-chiun Wang, and Wei-ting Liu, (2005)"Secure authentication scheme for session initiation protocol", Computers Security, Computers Security, pp:381-386.

[21] Eun-Jun Yoon, Kee-Young Yoo, Cheonshik Kim, You-Sik Hong, Minho Jo, and Hsiao-HwaChen,(2010)"A secure and efficient SIP authentication scheme for converged VoIP networksComputer Communications",Vol 33,pp:1674-1681.
[22] Fengjiao Wang and YuqingZhang, (2009)"A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography", Computer Standards and Interfaces,Vol 31,Issues-2,pp:286-291,.
[23] Yi-Pin Liao and Shuenn-ShyangWang,(2010)"A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves", Computer Communications, Vol-33,Issue-3,pp:372-380.
[24] Aircrak-ng. Available on: "http://www.aircrackng.org/doku.php".
[25] istumbler. Available on: "http://istumbler.net/".
[26] Kismac-ng. Available on: "http://http://kismac-ng.org".
[27] Kismet. Available on: "http://www.kismetwireless.net/".
[28] Macstumbler. Available on: "http://www.macstumbler.com/".
[29] Wireshark. Available on: "http://www.wireshark.org/".
[30] Patrick Studei, Marcel Bihr, Alan remund and Gustavo Alonso,(2007) "SIPHoc: Efficient SIP middleware for ad hoc networks". In proceedings of the ACM/IFIP/USENIX 2007 International Conference on Middleware, Middleware'07, pp: 60-79.

8. Conclusion

SIP security in Ad-Hoc network is proposed using SSAS algorithm with social paradigm. Security parameters are exchanged through online to prevent attacks. Every SIP message is signed with private key of user and attached with SSAS digital signature and SSAS address for authentication and message integrity. This technique gives Un-Spoof able address using SSAS algorithm. In this scenario, initial phase authentication is applied for new joining nodes before communication established. The simulation result reduces level of packet drop with increased range of various parameters like packet dropped ratio, session establishment time, mean end to end delay, average jitter and data transmission rate are compared with both enabled security features and disabled security features environment. The proposed algorithm gives better performance with unsecured environment.

Authors Bibliography

K.Shanmuga Priya received her B.Tech degree in Information Technology from BCET, Karaikal in 2010 and Completed M.Tech degree in Network and Internet Engineering from Pondicherry University, Pondicherry. Her research interest in Wireless Security and Cloud Computing.

P.Shanthi Bala, Assistant Professor, Department of Computer Science, Pondicherry University, Puducherry, received her postgraduate from Pondicherry Engineering College, Pondicherry. Her research interests include Artificial intelligence, Ontology and Networks. She is doing her research in the area of Reasoning. She has published 10 research papers in peer reviewed journal and conferences.