An Efficient Signature Scheme for Securing Multicast Communication

R.Krishnaveni National Engineering College Kovilpatti

ABSTRACT

Multicasting is an efficient communication mechanism for group oriented applications such as video conferencing, distance learning etc. Assuring certain level of security over multicast communication has become vital in Internet applications. Various cryptographic algorithms have been used to provide different security services. One among the cryptographic scheme is the digital signature which ensures authentication, message integrity and sender non repudiation. Digital signature algorithm such as RSA/DSA with SHA-1 can be used. In order to prevent passive attack, confidentiality has to be ensured. Confidentiality can be achieved by using the symmetric key encryption approach. The main objective of this paper is to provide all the above security services with low communication overhead. RSA with SHA-1 is one of the efficient public key cryptographic algorithms to provide security and therefore, its efficient hardware implementation is of great importance. This paper also proposes the design of SHA-1 implementation in FPGA.

Keywords

Authentication, client, confidentiality, encryption, server, verification

1. INTRODUCTION

Wireless networks have become increasingly popular in the communication industry. In emergency applications such as rescue and mission and military applications, there is a need to deploy a wireless network that can be formed instantly. Adhoc network is one such type of network. Ad-hoc networks are autonomous networks comprised of wireless mobile devices. Exchange of sensitive information over access paid services and unprotected wireless links demand the deployment of security in wireless networks. In recent years, secure communication has become an important subject of research. The main security service for wireless network is to provide confidentiality, authentication, authorization and data integrity. Most of the group oriented applications are based on multicast communication. Multicasting is an efficient method to deliver data from a sender to a group of receivers.

Secure data over multicast communication is a challenging task. In this paper, the problem of secure multicast of data streams over wireless ad hoc network is addressed.

This paper deals with the schemes for securing multicast communication and its implementation. In this paper, issues in multicast security and security services and the multicast scenario are briefly explained in section no.2. Algorithms used in the signature scheme are presented in section no.3. The basic digital signature scheme is discussed in section no.4. In section no.5, the proposed scheme providing N.Shanthi National Engineering College Kovilpatti

confidentiality is explained. The implementation of the multicast server and client and their results are given in section no.6.1, 6.2 and 6.3. The hardware implementation of SHA-1 is shown under subsection no.6.4. The pros and cons of the schemes are discussed in section no.6.5. Finally the paper is concluded in section no.7.

2. MULTICAST SECURITY

In the multicast communication, groups are identified by a group address (multicast address), and any node of the network may join or leave the group freely. So, membership in a multicast group is dynamic, allowing any hosts to enter and leave the multicast session without the permission or knowledge of other hosts. This inherent benefit of multicast communication presents some vulnerability making it susceptible to attacks unless they are secured.

In the multicast model, senders may not be the members of the multicast group. This means that any host can send data to the multicast group [1]. Further, group members need to be able to verify that messages received are from the intended source. Multicast source authentication solutions are needed to provide this functionality. Another security issue in multicasting is that data sent to the group may transit via many insecure channels. Thus, eavesdropping opportunities are abundant [2].

Multicast communication need to be secured against threats through the application of several fundamental security services [24] which are discussed below:

- Data integrity: Each receiver should be able to assure that received packets have not been modified during transmissions.
- Data origin authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims.
- Non-repudiation: The sender of a packet should not be able to deny sending the packet to receivers in case there is a dispute between the sender and receivers.
- Confidentiality: Data should not be made available to the unauthorized users.

The first three security services can be provided by the asymmetric encryption techniques called digital signature as in [3]. The sender generates a signature for each data with its private key (PR), which is called signing process, and each receiver checks the validity of the signature with the sender's public key (PU), which is called verification process. If the verification succeeds, the receiver knows that the data is authentic. Confidentiality can be achieved by using symmetric encryption technique.

3. ALGORITHM

3.1 SHA-1

SHA-1 (Secure Hash Algorithm) [19] has been widely used to provide message integrity. SHA-1 gets an input message smaller than 2^{64} bit and performs message padding by dividing the message into 512 bit blocks. Five 32-bit buffers are used which are initialized with the predefined value. These five buffers (160-bit) are used to hold the intermediate and final results of hash function. Each message block (x_i) is processed in four stages and each stage consists of 20 steps of operation as shown in Figure 1 [20]. The algorithm computes a 32-bit word W_0 , W_1 ... W_{79} for each of the 80 steps from the message block itself.



Fig 1: SHA-1 Compression function for a single 512-bit block

The words W_j are derived from the 512-bit message block as given in Equation (1),

$$W_{j} = \begin{cases} x_{i}^{(j)}, 0 \le j \le 15 \\ \left(W_{j-16} \oplus W_{j-14} \oplus W_{j-8} \oplus W_{j-3} \right) < <<1, 16 \le j \le 79 \end{cases}$$
(1)

where x<<<n indicates a circular left shift of the word x by n bit positions and j denotes the current step of operation.

The four SHA-1 stages have a similar structure but use different internal functions f_t and constants k_t , where $1 \le t \le 4$. Message blocks are processed by the function together with some stage dependent k_t . The output after 80 stages is obtained by adding to the input value H_{i-1} modulo 2^{32} in wordwise fashion. The operation within step j in stage t is given by Equation (2),

$$A \leftarrow E + f_t(B, C, D) + (A <<<5) + W_j + K_t$$

$$B \leftarrow A,$$

$$C \leftarrow B <<<30$$

$$D \leftarrow C$$

$$E \leftarrow D$$
(2)

Table 1 shows the definition of f_t in each step. The logical operators (AND, OR, NOT, XOR) are represented by the symbols (^, v, -, \oplus) respectively.

Step	Function	Function value
	Name	
0 <u>≤</u> t≤19	$f_1(B,C,D)$	$(B^{C})v(B^{D})$
20≤t≤39	$f_2(B,C,D)$	$B \oplus C \oplus D$
40 <u>≤</u> t≤59	$f_3(B,C,D)$	$(B^{C})\nu(B^{D})\nu(C^{D})$
60≤t≤79	f ₄ (B,C,D)	$B \oplus C \oplus D$

3.2 RSA

RSA is a very popular asymmetric key cryptographic algorithm used in many security protocols [14] [20]. In order to use RSA, a sender chooses two large random primes p and q to get N = p imes q, and then calculates two exponents e and d such that $e \times d = 1 \mod \Phi(\mathbf{N})$, where $\Phi(\mathbf{N}) = (p-1)$ (q-1). The sender publishes (e, N) as its public key and keeps d in secret as its private key. A signature of a message M can be generated as $\sigma = (h(m))^d \mod N$, where h(.) is a collision-resistant hash function. The sender sends $\{M, \sigma\}$ to a receiver that can verify the authenticity of the message by checking $\sigma^e = h(m) \mod N$. The strength of the algorithm is based on the difficulty of factoring numbers into prime factors.

4. BASIC SCHEME

The target is to authenticate multicast streams from a sender to multiple receivers. The sender signs each packet with a signature and transmits it to multiple receivers. Each receiver needs to assure that the received packets are really from the sender (authenticity) and the sender cannot deny the signing operation (non-repudiation) by verifying the corresponding signatures.

The Sender (A) generates the message (M) which is given as input to the hash algorithm (H) such as SHA-1. The output message digest value is encrypted using the private key of the sender and now the encrypted output serves as a digital signature. The signature is concatenated with the original message and it is sent to the receiver. The receiver (B), on obtaining the signature and message, perform the verification process. Receiver calculates the message digest value for the received message and decrypts the signature using the public key of the sender. Then, receiver compares the hash value and decrypted output as shown in Figure 2. If both match, the receiver knows that the message has not been modified during transmission (data integrity) and message is authentic.



Fig 2: Digital signature signing and verification process

This scheme [14] provides digital signature because only the sender could have produced the encrypted hash code. Public key encryption algorithm such as RSA, DSA can be used for signing and verification process.

5. PROPOSED SCHEME

The above digital signature scheme does not provide confidentiality since the message (M) is transmitted in clear. If confidentiality as well as digital signature is desired, then the message plus the private-key-encrypted hash code can again be encrypted using a symmetric secret key [20]. Then, encrypted message is transmitted to the receiver. The receiver decrypts the received message using the shared secret key (K). The decrypted message is then verified using the public key (PU) of the sender as shown in Figure 3.



Fig 3: Scheme providing authentication and confidentiality

The secret key can be produced using DES algorithm. For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output.

6. IMPLEMENTATION

In order to prevent unauthorized users from accessing the data, the server signs the data using digital signature scheme such as RSA with SHA-1 before transmission. The client can verify the authenticity of the message by using the verification process. Key size of 1024 bits is used. The scheme is implemented in Java [18], [21]. One server and four clients are used for implementation. Implementation of basic scheme and proposed scheme are given in results-I and II subsection.

The simulation of SHA-1 [15] algorithm is shown in result – III subsection.

6.1 Multicast Server and Client

When a host wants to send data to a multicast group, it puts that data in multicast datagram [23], which is a UDP datagram addressed to a multicast group. Multicast data is sent via UDP, which, though unreliable, can be as much as three times faster than data sent via connection-oriented TCP. Once the data has been buffered out and packetized, the sending host launches the datagram onto the Internet. If any client wants to receive data from a particular multicast group, it should join that multicast group. The receiving host must also be listening on the proper port and be ready to process the datagram when it arrives.

6.2 Results-I

The server generates the RSA key pair and calculates the digital signature and then packetizes the digital signature and sent to the client as shown in Figure 4. The reception of datagram packet by the multicast client is explained in Fig.5. The client whoever joins that particular multicast group can be able to receive the datagram packet. The client retrieves the public key of the server from the publicly available file and then verifies the signature.

Administrator: C:\Windows\system32\cmd.exe	×
G:\Program Files\Java\jdk1.7.0\bin>java MSender1	-
Private Key	
SUN KSH private CKI KEY, 1024 bits	20005107
	AE0003177
36520296894351645518080301182551562301045370908852650327633453836326785	90307912
50930284540100929191521015249808285203019526914993322352628503304059965	13182320
38629883	10100010
public exponent: 65537	
private exponent: 6428491966108265841162131412950592402998290587626843	25695655
210136514554808300751543253650089462811027381319347725877464378685048311	72691358
511807047133359040852001101231389543724528801800372504848690897642124993	54447899
378623235979358901207927768818042513956393928489525575929165136788810306	68710729
19147073	
prime p: 1306191611595697252537339487359379496328503879298571	14137224
L45107222538158287077755077755075783120577469201053227097307160973344045	63400245
12220471/200101 022709000000000000000000000000000000000	6 2076 676
prime g. 7273070800000000000000000000000000000000	149990022
3017997190717772713700112777920772131077307703797193118316826637235179836 589364879292583	1-1770022
00700707222303	41814116
38851244292075861888510798948853040176158824351312860923055934969231	08937406
65419950284023	00101100
prime exponent g: 6795723488343998756895008895077814447673573088824045	02575554
757068698016020528057799541601509339395394677866774610647476971686163549	62976487
27770073979907	
crt coefficient: 5904927758387484091924159514777103664488459164655564	80120090
J54505774808099165534878964874458363036181232167830983361237260605571559	15744095
34563836198173	
PUBLIC Key	
	24525200
M0001005 121147740520766223361722746752173766010406516661706266661771	34537374
70700434207320313474377123030733374001202371270700707707340303473437771703	50930794
57133161331666696116233136236191337676663263632763373363636267637636776367	38620883
1010077171371013247000203703017320714773372337070303304037703131023702	30020003
public exponent; 65537	
Encrypted Data (Packet) Sent	
Encrypted Data (Facket) Sent	
Encrypted Data (racket) Sent	
Encrypted Data (Tachet) Sent	
Cherypten Data (Inchet) cont	

Fig 4: Multicast server

🔤 Administrator: C:\Windows\system32\cmd.exe	<u> </u>
C:\Program Files\Java\jdk1.7.0\bin>java MReceiver1	^
Public key Received	
Sun RSA public key, 1024 bits	
modulus: 121147940528766223381712274675219396801040651668190828885197134	537372
76966434209326515474599123856753594861262391278706976934058549345999176336	520296
89435164551808030118255156230104537090885265032763345383632678590307912950	930784
54010097919157101524980828570301952691499337235767850330405996513182370238	620883
public exponent: 65537	
Encrypted Data Received:U!!inx=]'XYX2:Ell&dT¶Ug <_U`ù'XY=êôï-Ö !!SUÂS'o@5+Û: Am=YAÇ Û*'íőàî!@8#A[Ss_2xxxp^o!¥i=] \1	} † ∟⁄2
Message(Original Data)Received	
Java is a pure object oriented language.It is widely used in Networking be of its security features.It does not support pointers.Java is simple to co platform independent.Morever,Java is robust and it supports Multithreading	cause npile, ,inher
itance and packages.	
signature verifies: true	<u> </u>

Fig 5: Multicast client

6.3 Results-II

To provide secure transmission in multicast communication, a new scheme is proposed which encrypts the signature before transmission and decrypts the encrypted signature after reception. The multicast server generates the RSA key pair and DES secret key and encrypts the digital signature using the secret key which is observed in Figure 6. Then the encrypted data is packetized and transmitted to the requested client. On receiving the datagram packet, multicast clients decrypts the received data and then verifies the decrypted data using the public key of the sender as inferred from Figure 7.

<pre>(:\Program File:\Jaux\jdk1.7.0\bin\java MulticastSender Private Key Sun RS0 private CRT key, 1024 bits modulus: 1231866145929245227554393611976713701631534398843497814996 82382259337736661836157016372785582180285313497802519859901646452077894737837946 825787042625202232806106039656464685716976841817332808073824642265494191397808395446 5355226527803 public exponent: 65537 private exponent: 45537 24523078071495645731572221867324158299230833231641756822560765929931325607169859 654576183483819572565800299014698943197819477212549085726604629009128668780217260 97895985 priva te exponent: 45537 private support: 1242240963305615588439878050802758393671723366897784747473288897 654576183483819572565800299014698943197819477212549085726604629009128668780217260 97895985 prime p: 12422409633056155884398783084795839677172336653745747475328827 966867477901327 prime q: 99165822575711911588219755776176119718131198631446691866554381055584186777755 6413371407850433163131546731427364482147274610490907498013887015360865138186777755 754138299108498852275579119115882197557761761197181311986314669138665158186777755 754138297001327 prime q: 99165822517808940822142746119546865262633955944155160855858186777755 75413827910843981522257 9718642332229 prime exponent p: 46941872408923355946431264051316946316322787856818677775 543387240725048315315467314273644821472746104990974980138870153608651391851542 55343827001943 prime exponent p: 499112198712793754215951464312446319780965225439318556818677775 5413872408723408244458875053259555935564515743892441771314 5265530780643335191438214746213932861895595356463126405310980965225439318754972 5533827001943</pre>	Administrator: C:\Windows\system32\cmd.exe	_ 🗆 X
Private Key Sun RSA private CRT key, 1024 bits modulus: 12318864145939245227554393611976713706631534398843497814996 83252937736661836157081537252108253134798025198590616455287789473708395416 5355208275893395969086646108379495792390425121473602226075529031256071639859 public exponent: 1245852490730517175317201087156691508528539878508029750839671723608937457417328829 545520873297985 private exponent: 124224896330561558842953387850802975083957123369453255290897561238227 private exponent: 124224896330561558842973308322164175602226075529031256071639859 2452309786517175317201087156691508558253878508029750839571723608957457417328829 545576104483105725556080290146099734137074977212549885725607552931725687163821726 970957985 prime q: 1242248963305615588429633854786859488183553580295937921517187 13827910884908522755791194115882197557761761117181311986314466918669543818522439 0668874779240843163135467314273644821472746140490974798138874153608613918515426 6488842332229 prime q: 9716582317809403335619486214421472746140490974798138874153608613918515426 648884232227 prime exponent q: 999152219871279375421959146463173729009367377633877453897349529378 553438274802444887533272788274482748219375577139141159821975575 807765123237308043335619438274133266073927542195914646317372900936737763387349529378 55343827480244421472746149897493293557555580937541157713445824568355554515743892241777154 4526538780733 prime exponent q: 9991221987127937542195914645317872909367377633873497582239786311975713763187729093673469754837346575 57833748173487248824445793248224476453487882127278537488744872392641727461314584247678478478672472893674487593248254973 prime exponent q: 9999122198712735521990552375809735411945842456835555454557438922441771314 4526538788733 prime exponent q: 1989812219872553938666437897147979748757544872478978487789779346857448757837948757897794687594627897794678794678794678797946875946878973974685794678797974685794687897897979468759467897785748878978979468579467878977946875979468789189999645454545	C:\Program Files\Java\jdk1.7.0\bin>java MulticastSender	
Sun RSB private CRT key, 1024 bits modulus: 1231886414593924522275543936119767137061631534398843497814996 823822593377366618361570816372785582108285313497802619859981646452077894737087946 827872462625223238611608386564616633704957123280807382164242694419379813897461 53553285372853728933995980664610633704957123280807382164242694544137038087945 private exponent: 12458244383653382572322584320353389450825529809756123832454 private exponent: 124582244383653382572322584320353389450825529809756123832454 private exponent: 124582244383653382572322584328353389450825529809756123832454 786537914854673157222186732415827923808275838577123858373474175328827 245289780617175317281089715641280752655080827961385427863854771753624801825552978721517187 78659791485461361577256550808293145954219353564275838547173286827771238537474175328827 64545798448330195725655080293145987431578012753584741553808275808754612539809755127869 Prime : 9115822375577119411588219755776176119718131198631446691866954301855254395977255 4113871407850483163131546731427364482147274618498987498813887081556086558568186777755 646897477920483143313154673142736448214727461499898749881388708153608613918651568 796213273980433358194382147462139328618959523856818942913566861392637559441551685585888677755 87762132739804333581943821474621393286189595238568189421361632727858271893708612 5343827001943 prime exponent p: 98918221987129375421959464312732749683555954515743892441771314 4526538788733 crt coeff cicent: 1080360966995539387089375419450482496835559545157433972495121932329 7983314411873481 Public key Sun R88 public key, 1024 bits modulus: 123188641459392452275543936119767137081631534398843497814996823825953 272662186493636746457149724822275543936119767137081631534398843497814996823822593 37756618315704163277495821898265314978041157712412336836355954411388265267883 public exponent: 65537 Secret Keycom, sun crypto, provider. DESKeyE185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data	Private Key	_
monulus: 12318864145732225222254393611797671378154479881497541378815784 s238225933773666183615781637280521080255134797886210897531246164532578914644528727847378817946 87578462657282232866116083863664685716776841817332888073824652422694419378813853554411388 255528637580339509698664610637945189279239461666847809189999458466334583555411388 25527883 public exponent: 1245852443836533812572322584328353389458255298097561238322454 7886378149854657315722216673221158279239461323216417568222697657283316717353122688732822 245238978651717531728188715661580558253878580277583856717234695375457417332827 prime p: 124224896338581558842963385478685948818355358295937921517187 1382791808398522755791194115882179557741761197181311986314466918667543818522349 866897477981327 prime q: prime q: 9915229735479194215882179557474611999879499813887415316858568186777755 4713971467584831631154673142736449221472246189989749981388741531686138978153468613918515426 6548834232229 prime q: prime q: 99121299712793754129514464313729809327977632872783827989727898721997931282 8533423229 parine q: 95435597724882348648535585325655788937541197671378163153498833794952839786152 80730577234892349789121997127973754215914645137929893278785937897979897815 9736569787248924	Sun RSA private CRT key, 1024 bits	
B2382233377380813615748832785 B25784225278232328616803865646857115766181737328888738264622654411338 B5784242527823238616803865465837949579239461666647891899945346683458535441138 Public exponent: 124585244383653382572322584298353394582523988975612382444 B85378744625278272316773415829723082371441756822269755293125687169859 Public exponent: 124585244383653382572322584298353394582552988975612382444 B853787446252757231726188715659158853825918785892756389571723469537457415328887382444 B853787446258751727531726188715659158853825918785892756389571723469537457415328887 24523897865171753172618871565915884256338547685574801452975989128688788217266 79695985 prime p: 1242249653815588429755761761197181311986314466918669543916522439 B66897477901327 prime q: 99165823517889488618195464312644851898985726604629809128688788272755 541387148785648316313154673142736482147274618498987498813887815364861591862555 B87962132739804333581943821474621393286189585238568189421361685585584818577755 541387148785648316313154697314273648214727461498987498813887915364861391861545 553438274081244887583322698375633245789335419458424468318987815364864518982355945157488274482147274614 564583473723488244458937583225578933541945814746213932861895238568618942136163227785827189378612 553438274081943 prime exponent q: 98981221897127937542195914646317372940893673776338734952857831374912 553438274081943 prime exponent q: 989812218971279375421959146463173729408936737753887349382241771314 45265530788733 cr coeff ci eint: 1108336096698653934879411577124129368335595451574837448254282789378 377566133615701632727858214082799245227554393611976713701631534398843497814996823822593 277566133615701632727858214082799245227554393611976713701631534398843497814996823825932219 7662541516944415397245822755493361947611577124129360336648679874413783887444153552853285 75993394814418392447279245822755493361497247942778379746373794687547842544825397 572482224861663165764646571857641181732280842447894741378248424477843779463747837946875478425478837394685	modulus: 1231886414593924522275543936119767137016315343988434978	14996
h:j:remission of the second se	82382257337730bb183815781637278582198283313477882617857781646452877674747378 09E78A22669825290241280362268768267674747378	06416
2662270803 public exponent: 165537 private exponent: 12458524430365338257232258432035330945025529080756123032454 private exponent: 12458524430365338257232258432035330945025529080756123032454 2452309706917175317201807156691500550259387850029756309571723405937457417338029 24523097069171753172018071565915005502593878500297563095726084529009128668708217260 279595905 prime p: 1242240953305015580429563305478665540813355356295937921517187 13822971080849085227557911941158821975577617611971813119863144669186695439180522439 066809477901327 prime q: 9916582351708094082810195466550263955944155169558568186777755 441387146785044316313154673142736448214727461049097490813887015360861391805154 2668094797273480244458875633226557581741415882197557761761197181311986314466913887053508655586153768555 897965213233980433358194382147462139326610950523856818942136168558568136777755 4413871467850443163131354673142736448214727461499097490813887015360861391805154 2565330872001943 prime exponent q: 90912219071279375421959146463117372900936737763307349528254381976612 55343827041943 prime exponent q: 90912219071279375421959146463173729009367377633073495380241771314 45265530788733 cr coefficient: 1080360960986539348704115771241293603366467895423382541279332297 7662543151694045124027792402853936664372091952447087621726481737327051219932329 793831441273181 Public Key Sun RS public key, 1024 bits modulus: 12318064145379245227554393611976713701631534398843497814996823822593 277566110631570166357697554111732210923245227554393611976713701631534398843497814996823822593 377566110631570166371570465514976411732200925554615374044153752109532249794675723094641565522653 57893339493866461083769746572379465245227554393611976713701631534398843497814996823822593 377566611361570166357165764111732210892452275543936119767137016315343988434978149968238255267883 public exponent: 65537 Secret Keycon sun copto provider .DESKey018564 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data	67579702057202252000100590030030030037107700101107320000750270272077117370030	111388
mulic exponent: 6537 private exponent: 14365244303653382572322584320335330945025529089756123082454 78053709140564573157222106732415829923003323164175682258075502993132560716508594 78053709140564573157225058002901450894319701947721254908572609452250978973674175320827 7805305717753172045073157255750175175015771230653737474175320827 78293906433055725658002901450804296330541558042963305470560547018045772356575751723068373747175320827 prime p: 124224096330551558442963305476618940113053596255947921517187 713299910849085227557191911580819755776176119718131198631446691865954301652245 7829910849085227557919411580819755776176119718131198631446691860555808186777755 6480834232229 prime exponent p: 9916582351708940822810129350464312640531090009522543081865055 78772140725043316313154673142736440229354563129350464312640531090009522543081865055 787721409293043335191438214746213932861895053285608189421361632727850827183970612 78736612319904335191438214746213932861895053285608189421361632727850827183970612 787366123199043351914382147462139328618959534516443173729009367373733873497528373 prime exponent p: 46941821408279127937542159312646312640531098090522543081797489737086121993229 78331441873181 Public key Sun R80 public key, 1024 bits modulus: 1231806414593924522275543936119767137016315343988434978149968238225733	265267883	11300
private exponent: 124585244393653382723225843203353394958252908975612382454 7865378914856457315722186734156915085502393878508029750339571723669750843125687169085 2452309766517175317201807156691500550259387850029750339571723669539734574173382829 54575613438319572556550029014690943197019477212549085726604629089128668780217260 97095985 prime p: 1242240963305015558042956338547868594018355356295937921517187 13822918084908522755791194115882197557761761197101311986314466918669543918622439 0668094777755 4113971467050431426132746442142724614049097490813887051350661391865556 0668094777275 41139714670504314631315467314273444214274261404990974908138870513506661391865555 06580947797273 4113971467045043146313744021392364109506238564109421361632727850827183970612 553438270401943 prime exponent p: 4091822198712793754219591464631737290093673776338734972409730976612 55343827041943 prime exponent p: 9091221987127937542195914646317372900936737763387349724073794057734974612 55343827041943 prime exponent p: 409122198712793754219591464631737290093673776338734974495733976612 553438270419733 prime exponent p: 4091822198756322657809375411454642317729409367376338734872441771314 91316 Rey 1824 91415 Key 1824 913165 12402277924026453393467	public exponent: 65537	
78863789148564573157222186732415829932803232164175682226875592893132568716399895 452330786717753128018971566158085253938768082756339671723665375474176328827 65457618348381957256558082901469894319781947721254988572688462989128688788217268 prime p: 124224896330561558842963385478685948818355358275937921517187 13829918884988522755791194115882197557761761197181311986314466918669543818555586186777755 44138714878564331631315467314273644821472746189498974980138878153686518661391861542 6648834232229 prime e: 9915582251788948828197557614949897498013887815366861391861542 6648834232229 prime exponent p: 46941873482736448214727461849897498013887815366865586186777755 54138791848248456433153131546731427364482147274618498974980138878153668613918615426 664883432229 prime exponent p: 4694187348927355941546317372986936594415163227878658518 B87562132739084333581943821474621393286189595544515463157329869367377633873499528375 85178356972734882444588756532555788937541945848249688355954515743892441771314 4526553878733 crt ceefficient: 180336066989653934874011577124129360336646678954233825932219 76362543151694451248279924828593366664372891952447887621726481737327851219932329 783831441873181 Public key sun R8n public key, 1824 bits modulus: 123188641459392452227554393611976713781631534398843497814996823822593 3773666136157816327279468253214827897946875704462 592822328641683363646465716976945134978842378978947397946875704462 592822328641683363646465716976945134978847389784678759446875944653 59282232864168336364646571697694181733288898738246242694419378383954411388265267883 public key. net keyonest: 65537 Secret keyonest: 8ent Encrypted Data (Packet) 8ent Encrypted Data (Packet) 8ent Encrypted Data (Packet) 8ent Encrypted Da	private exponent: 1245852443036533825723225843203353309450255290897561230	32454
2452309786517175317201807156591500550539378500227508396717236059374574173380229 545756124583155725550002201540943197019477212549085725004622909126808700217260 97095905 prime p: 124224896330561558842963385478665940818355350295937921517187 13829918084908522755791194115882197557761761197181311986314466918669543018522439 066807477981327 prime q: 9916582351708940828101954606502639559441551695856818677755 4133071467035040316313154673142736448214727461404909749081308704153606613910515426 664808342332229 prime q: 9916582351708940828101954606502639559441551695856818677755 413307146703504331631345473142736448214727461404909749081308704153606613910515426 664808342332229 prime exponent p: 469418734092935457031293594645316986093525243081380761350406219794919790412 55343827040954445087503325695709375421959146453173729009367377633073499520375 85778534727340824445087503325570937542195914645317372900936737763307543892441771314 45265530780733 prime exponent p: 109336096098653934870411577124129360336648670954233825932219 76625431516940512408279924028337366643720919524470876217254481737327051219373282997 77366153157416527475582100728131497086218959916444527679347946875044683759322593 773661531574165277558210072813149780211975713701531534398843497814996823825932219 766254315169463124082799240283373666437209195244708762172540824479748575044685 5989339441873181 Public key Sum B%n public key, 1024 bits public key, 1024 bits	788637891405646573157222186732415029923083232164175602226876592893132560716	98050
b-45/56/10/40/31195/225b5/00/22/01/45/99/317/2019/27/2125/9085/26084/62/9097226b87/02/1726b prime p: 12/4224896330501558842963385478665948618553580295937921517187 13829910/864908522755791194115882179755776176171197181311986314466918665438108523439 966887477981327 prime q: 9916582351708940828101954686502639559441551609558568186777755 4413871407050431231313154673142736448214727461049090749081388708133608613910815426 6488834232229 prime exponent p: 46941873409293545703129350464312640531098009522543031055555 807/621239390433350194382147462139328610950623856610942136163227805827183970612 55343827001943 prime exponent p: 40941873409293545703129350464312640531098009522543031056555 807/62123930643350194382147462139328610950523856610942136163227850827183970612 55343827001943 prime exponent g: 409912219871279375421959146463173729009367377633073499520375 8517033607273408244458875063325055708937541945048249688355954515743892441771314 452655307873 ert ceefficient: 100336096098653934670411577124129360336640670954233825932219 706254315169404512402799240285393660643372091952447087621726481737327051219932329 708381441873181 Public key sun R8A public key, 1024 bits modulus: 123180641453932465227554393611976713701631534398843497814996823822593 277366613615701632727495792390461666847089189990458466834585395441138265267883 public exponent: 65537 Secret keycon.sun.crypto.provider.DESkey018534 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sen	245230978691717531720180715669150055025938785002975038967172360593745741763	28829
7/073703 124224896330501558084296338547868594881835535825937921517187 138279100849052275579119411588219755776176119718131198631446691866754308625439 066807477961327 prime q: 97168034908522755791194115882197557761761197181311986314466918667543086523439 066807477961327 prime q: 971680340316311464731427364402214727461849909749081380708133060613918515426 064803423222 prime q: 97168034233229 prime q: 97168034233229 p: 9872803423228 p: 987280342328 p: 98728129081433561943821474621393266189565238560189421361632272785827130970612 98738129701491 q: 987323 q: 987333 q: 98731441873181 Public key Public key 1803366064053394870411577124129360336648670874233825932219 703831441873181 Public key Public key 180336957923904136664372091952447887621726481737327851219932329 703831441873181 public key Public key 18034459379452227554393611976713701531534398843497814996823822593 7736616315784153772585210602513149780579239046156684708971892789472789727897468757946875794687579468757946875794687579468757946875794687579468757946875794687579468757946875794687	654576103483817572565800270146787431770174772125470857260846270871286887802	17260
1382991 dBs 4908522755-6216411941158821975577617611971013119683144466918669543451622439 066897477961327 1919 dBs 4908522255-62164119411588219755776176119710131196831444669186695434516522439 066897477950648316313154673142736448214727461499987498013087015360861391051542 6648084779755 441307140705048316313154673142736448214727461499987498013087015360861391051542 6648084779755 97796213273980433350194382147462139328618950523856018942136163272785827183970612 55343827001943 prime exponent p: 909122199712793754219591464631737290093673776533073499524373 55343827001943 prime exponent p: 9091221997127937542195914646317372900936739776530873495241771314 45265530788733 crt coefficient: 10033609609653934870411577124129360336648670954233825932219 7662543151694051240279924028539366064372091952447887621726481737327051219932329 70833144173181 Public Key Sun R86 public key. 1024 bits modulus: 12318064145939245227554393611976713701631534398843497814996823822593 37736661036157016537270558210028531349708026193929464452077944773732746153552083 7589339969666410631679445512402799245227554393611976713701631534398843497814996823822593 3773666103815701653727055821002853134970802619392464452077944773732746153552083 758933948104038056485716570641817332208025534264265 5220222260160390563846571657054181733220802651949598016445207789473737946875594626 5220222264116393616394455124027992452227554393611976713701631534398843497814996823822593 3773666103815701653727858210028531349708026193998046453459754411338265267883 public exponent: 65537 Secret Keyom.sun.crypto.provider.DESKeyE185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet)	7/073703 	17197
B6688/2477901327 prime (:) 9916582351708994082811915466658263955944155160558568186777755 641387140708504331631315467314273644821472746104909074980138870153608613910515426 6488814232229 prime exponent p: 469418734087293545708129350646312243566018942136163272785685515 807902132739004333581943821474621393286189505238560189421361632727856827183970612 prime exponent p: 4999122190712793754219591464631737290093673776358373497528375 B517033507273408244458075053225055708937541945648249688355954515743802441771314 45265530708733 ert coefficient: 100336006096653334070411577124129360336648670054233825932219 7662543151694451240279924028539366064372091952447087621726481737327051219932329 703381441873181 Public key Sun R80 public key, 1024 bits modulus: 123180641459392452227554393611976713701631534398843497814996823822593 773661613157016327275582100282813149708213497084578947470897946975704685 572802322061608306364665716976974474981197332408073826424259441137083896416535532063 57280232220616083063646465571597684418173328080738264242594411373083896416535532063 75893399698064645657978974708977929946855308666854583954411388265267883 public exponent: 65537 Secret keycon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent<	13829910884908522755791194115882197557761197181311986314466918669186695430105	22439
prime 99165823517889468218119564665263955944155169559568186777755 441387146796483163131546731427364482147274610490974980138870153608613918515426 6648834232229 prime exponent 65213273980433350194382147462139328618950523856018942136163252543031856855 87962132739804433350194382147462139328618950523856018942136163272785827183970612 553438270401943 prime exponent cstopped prime exponent cstopped prime exponent cstopped prime exponent cstopped prime prime exponent cstopped prime prime exponent cstopped prime prime exponent primolus prime<	066887477901327	
441387146785643163131546731427364482147274618498974988138878153668613918515426 66488834232229 prime exponent p: 4694187348929354578312935846431264953189880952254381865855 897962123973980433358194382147462139328618959523856818942136163272785827183978612 55343827001943 prime exponent q: 989812219871279375421959146463173729069367377633873499528375 8517835697273480244445887565325585788937541945948249688355954515743892441771314 4526553878733 crt coefficient: 108036096698653934870411577124129360336648678954233825932219 7662543151694051248279924828539366664372891952447887621726481737327051219932329 783831441873181 Public Key Sun R&A public key, 1024 bits modulus: 123188641459392452227554393611976713701631534398843497814996823822593 37736661361578163272949579239046166684780918909045846683458789472637946875704625 55282232664166833663646465716976945134978824382646535532865 7889239949806646108579457923940451668478091890904584668345853954411388265267883 public exponent: 65537 Secret Keycom, sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted	prime q: 9916582351708940828101954686502639559441551605585681865	77755
6648834232229 prime exponent p: 469418734892935457831293584643126485318980895225438318568555 887%62132939804333581943821474621393286189585238568189421361632727858027183976812 55343827081943 prime exponent q: 9898122198712793754219591464631737290693673776338073499520375 8517035672734802444588758532269557893754194548245688355954515743892441771314 45265530788733 cr cceficient: 1080360960986539348704115771241293603366486709542338254177134 45265530788733 prime exponent q: 98981221982428539366064372091952447887621726481737327051219932329 7862543151694045124027924028539366064372091952447887621726481737327051219932329 78631441873181 Public Key Sun RSA public key, 1824 bits modulus: 1231886414593924522275543936119767137061531534398843497814996823822593 377366518361457816537270558210028531397082619859901644528774974837946875704625 7280223206166384616385716576418173320809730246224524254541137081631534498843464528778465379468575916426 572822232616638461636571657641817332808738246524524574137783746875764265 5728222326166384616385716576418173328087382465245245741413789884349781497814535528633 920512 exponent: 65577 Secret Keynon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Pac	41387140705048316313154673142736448214727461049090749801388701536086139105	15426
prime exponent p: 46941073409293457040929345704072934676312735046431226406531264095225430310650555 0877621237309043335017438214746213733726105820538560109421316163227850827183370612 553438270611943 prime exponent q: 989812219871279375421959146463173729069367377633073499520375 85170336507273408244458875063325655708937541945048249688355954515743892441771314 452655307887733 ert ceefficient: 10033609669865393487041157712412936033664067095423825932219 7662543151694051240279924028539366064372091952447087621726481737327051219932329 708381441873181 Public key Sun R&A public key, 1024 bits modulus: 123180641459392452227554393611976713701631534398843497814996823822593 7736661361570163272794057923904616668470891890904584668345853954411388265267883 public exponent: 65537 Secret keycom.sun.crypto.provider.DESkey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	66488834232229	
be 7A5213273900433350174382147452139328610495052385010974213615272760507183770612 55343827001943 prime exponent q: 909012219071279375421959146463173729009367377633073499520375 B5170353672733 crt coefficient: 1003360960906539340704115771241293608365468678954233825932219 76625431516540631240279924028539366064372091952447087621726401737327051219932329 708331441873181 Public key Sum RN public key, 1024 bits Sum RN public key, 1024 bits T773661615791652772558210002513149706713701631534390843497014996823022593 77736616157016327735582100025131497062130990458466834507394740875704685 5920222060160830636464657197504181733200097302645242667441937003096416535532065 59202220601608306364646571975970418173200097302645242667441937003096416535532065 5920222060160830636464657957923304616668470091189090458466834505354411308265267083 public exponent: 65537 Secret Keycom.sum.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet)	prime exponent p: 469418734092935457031293504643126405310980095225430310	68555
<pre>S353627001743 prime cxponent q: 9098122198712793754219591464631737290809367377633873499528375 B51783567727340824445887508322505570893754194508249668355954515743892441771314 452653207827340827433 crt coefficient: 100336096098653934606413727124129360336648678054233822919 7662543151694051240279240285393660643722091952447687621726481737327051219932329 703831441873181 Public key, 1024 bits modulus: 12318064145932452227554393611976713701631534398843497814996823822593 7773666136157016372749749792394641653453208087382646452459441193708396416535532063 public key. 1024 bits modulus: 1231806414593245227554393611976713701631534398843497814996823822593 773666136157016372749475821002853134978026190599016464524759474780379464755704626 572022320601608306368464657169760418173320808738264624269441937083896416535532063 public exponent: 65537 Secret keycom.sun.crypto.provider.DESKey010534 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent</pre>	087962132737804333501743821474621373286187505238560187421361632727850271835	70612
bs1783569727348824445687566332250657089537541945048249688356954515743892441771314 ds26553078733 tc coefficient: 109336096096639653934070411577124129360336648670954233825932219 7652543151694451240279924028539366064372091952447887621726481737327051219932329 703831441873181 Public key Sun RS0 public key, 1024 bits modulus: 123180641459392452227554393611976713701631534398843497814996823822593 77366613615704153727558210802831349708613959901644545278794672637946875794625 592822212664160830636846457159758418173328080738254524259441937083896416535532053 75893399659066451063794957923904616668470891890904584668345853954411388265267883 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted	ps34302/001745 pwime_exponent_g: 9898122198712703754219591464631737290009367377633073490	20375
45265539789733 crt coefficient: 100336096098653934870411577124129360336648670054233825932219 76625431516940451240279924028539366064372091952447887621726481737327051219932329 703831441873181 Public Key Sun RSA public key, 1024 bits modulus: 12218864459739245222755439361197671370165153439080434970814996823822593 377366613031570163727055821002853134970802619859901646452077894737037946875704626 5728223286016033065304665716976041817332080073820465426247694419370833954165335520853 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey01854 Encrypted Data (Packet) Sent Encrypted Data (85178356972734082444458875053225055708937541945048249688355954515743892441	71314
crt coeficient: 10033609609663953934070411577124129360336640670954233825932219 7652531516940512402799240285393660643720919524470876217264017373270651219932329 703831441873181 Public key Sun RSA public key. 1024 bits modulus: 123180641459392452227554393611976713701631534398043497014996823822573 377366613615701632726758210026251349708021695990164452877894737037946975704625 5920223206016083063604646571697604181733280809738264524259441937083896416535532065 59202232060160830636046457169769418173328080738264524259441937083896416535532065 5920223206016083063604645797023904616668470891090904584668345853954411388265267083 public exponent: 65537 Secret Keycom.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	45265530788733	
766254315169404512402799240285393660643720919524478076217264817373270551219932329 708331441873181 Public Key Sum RSA public key, 1024 bits modulus: 123188641459392452227554393611976713701631534398843497814996823822593 37736661035157016392785582100828531349780261985990164452072894770837946875594656 572022228061680896366464685716575641817332808973826462425444139708389544153353 758933996980664610637979457923904616668470891898904584668345053954411308265267883 public exponent: 65537 Secret Keycom.sum.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	crt coefficient: 1003360960986539348704115771241293603366486709542338259	32219
703331441873181 Public Key Sun R&A public key, 1024 bits modulus: 123180641459392452227554393611976713701631534398043497814996823822593 37736661383157016327255821002853134978026198599016464520778947370837946875704626 57202232060160830663608470879269418173320800738264524269441937083896416535532063 7593339769806645108379457923904616668470891890904584660345853954411388265267883 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	766254315169484512402799240285393660643720919524478876217264817373270512199	32329
Public Key Sun RSA public key, 1024 bits modulus: 123188641459392452227554393611976713701631534398843497814996823822593 37736651836157016572705582100285313497080261985990164452077094737083794687549764626 57202232806160308636436458716976418173320806730264224524741370830784416535520853 758933996986646108537949579230966166604708971090904584668345053954411308265267083 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey@185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	703831441873181	
Funito Rey Sun RSA public key, 1024 bits modulus: 123180641459392452275543936119767137016315343980434970814996823822593 377366613815701632724558210028531349700261985901646452077894737037946475704626 59202232060160830636046857169766418173320000738264624269441937003396416535532063 758933930690806645108379495792390461666847009189090945846603450853954411388265267083 public exponent: 65537 Secret keycon.sun.crypto.provider.DESKey01854 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Duble Version	
" ""	Fublic Key Sup PSA public key 1024 bits	
177366611351570705587100820531349708026198599016464520779947278379468757994626 15720222326610638963646468571657764181733280942544137030879468755784616535532065 157202223266106389636464685716577641817332809473826424245441370308794541535532065 1572022326646106379794579239846166668470891898994584668345053954411308265267883 public exponent: 65537 Secret Reycom.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent	modulus: 1/2318864145939/4522275543936119767137016315343988434978149968238	22593
592822226616833663644657169766418173228086738224529441937083896416535532063 758933996980646108379495792390461666870891890904584668345853954411388265267883 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	37736661836157016372785582100285313497802619859901646452077894737037946875	04626
758933996986664618637949579239846166684788918989845884668345853954411388265267883 public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey0185a4 Encrypted Data (Packet) Sent Encrypted	59202232860160830636846857169768418173328080738264624269441937083896416535	32053
public exponent: 65537 Secret Keycon.sun.crypto.provider.DESKey@185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	758933996980664610637949579239046166684708918909045846683458539544113882652	67883
public exponent: 5537 Secret Keycon.sun.crypto.provider.DESKey@185a4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent		
secret Reycon.sum.crypto.provlder.DESReyCluSa4 Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	public exponent: 65537	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	pecret Reycom.sun.crypto.provider.DESRey@185a4	
Encrypted Data (Aachet) sent Encrypted Data (Aachet) Sent	Encrypted Data (racket) sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Tacket) Sent	
Encryfied Data (Packet) Sent Encryfied Data (Packet) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Packet) Sent	
Incrypted Jata (Tacket) Sent Encrypted Jata (Tacket) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent Encrypted Data (Packet) Sent	Encrypted Data (Packet) Sent	
Encrypted Data (Packet) Sent	Encrupted Data (Packet) Sent	
	Encrypted Data (Packet) Sent	

Fig 6: Multicast server

🖼 Administrator: C:\Windows\system32\cmd.exe	_ 🗆 X
C:\Program Files\Java\idk1.7.0\bin\iava MulticastReceiver1	
Public kev Received	
Sun RSA public key. 1024 bits	
nodulus: 123188641459392452227554393611976713701631534398843497814996823	822593
37736661836157016372785582100285313497802619859901646452077894737037946875	704626
59202232860160830636846857169768418173328080738264624269441937083896416535	532053
75893399698066461063794957923904616668470891890904584668345853954411388265	267883
public exponent: 65537	
Decret Rey	
CON.SUN.CTYPTO.PTOVIGET.DESKEVEI8584 To sound al Data Data in 1. 1. 4/2104 (201) and 1/4.Destruk (14.00200) is 05270-1400	1_ 172
Encrypted Data Received:	-11 XII
RN°DD/% F="COPEISN">)VOKICUTIU\W EN@'O&'%7272, FD%V	
nessage(vriginal Data/Received	
pava is a pure object oriented language.it is widely used in Metworking be of its security features.It does not support pointers.Java is simple to co platform independent.Morever,Java is robust and it supports Multithreading	rause mpile, f,inher
itance and packages.	
signature verifies: true	
Civ December 1721	-
h:/rrogram/riles/wava/jakl./.u/bin/	

Fig 7: Multicast Client

6.4 Results-III

The module for SHA-1 is written in verilog and simulated using Active HDL. The timing waveform obtained during simulation is shown in Figure 8. The module is synthesized using Quartus-II software and the compilation report is given in Figure 9.



Fig 8: HDL simulation result for SHA-1

ummary			
Flow Status	Successful -	Tue Feb 28 13:45:26 2012	
Quartus II Version	8.1 Build 163	10/28/2008 SJ Web Edition	
Revision Name	sha15		
Top-level Entity N	ame sha15		
Family	Cuclone II		
Device	EP2C35F672	XC6	
Timina Models	Final		
Met timina require	ments N/A		
Total lonic eleme	nts 40.977		
Total combinal	ional functions 40.977		
Derficated Inni	renisters 5.636		
Total registers	5636		
Total nine	386		
Total virtual nins	0		
Total memory bits	ů		
Finherderd Multin	ier9.hitelementeΩ		
Total PU .	П		
TOIGHTELS	0		

Fig 9: Compilation report for SHA-1 module

6.5 Discussion

Here server is one of the members of a particular multicast group and uses RSA with SHA-1 algorithm to provide the desired security services. Since SHA-1 produces a fixed output of 160 bits, communication overhead is reduced. Since there is no relationship among packets and each packet can be independently verifiable, this scheme reduces authentication latency. But the sender needs to sign each packet which costs more computation overhead. However the sender is usually a powerful server and so per packet signature generation can be affordable.

In hardware implementation of SHA-1, one clock cycle is spent for each step of operation. For each block of data, hash value is obtained at the end of every 80th clock cycle.

7. CONCLUSION

Multicast enables efficient large-scale content distribution by providing an efficient transport mechanism for one-to-many and many-to-many communication. The properties that make multicast attractive, however, also make it a challenging environment to support Internet-based applications. To solve the security issue in multicast environment, various encryption techniques has been employed. In this paper, we have presented some security schemes for multicast communication. Secret key management issue has yet to be considered. Hardware implementation of RSA is yet to be implemented in future.

8. REFERENCES

- Judge, P., and Ammar, M. 2003. Security Issues and Solutions in Mulicast Content Distribution: A Survey, *IEEE Network Magazine*: 30-36.
- [2] Challal, Y., Bettahar, H., and Bouabdallah, A. 2004. A Taxonomy of Multicast Data Origin Authentication: Issues and Solutions, *IEEE Comm. Surveys & Tutorials*: 34-57.
- [3] Zhou, Y., and Fang, Y. 2007. Multimedia Broadcast Authentication Based on Batch Signature, *IEEE Comm. Magazine*: 72-77.
- [4] Even, S., Goldreich, O., and Micali, S. On-Line/Offline Digital Signatures, *J. Cryptology*: 35-67, 1996.
- [5] Perrig, A., Canetti, R., Tygar, J.D., and Song, D. 2000. Efficient Authentication and Signing of Multicast Streams over Lossy Channels, *Proc. IEEE Symp. Security and Privacy (SP '00)*: 56-75.
- [6] Pannetrat, A., and Molva, R. 2002. Authenticating Real Time Packet Streams and Multicasts, *Proc. Seventh IEEE Int'l Symp. Computers and Comm. (ISCC '02)*: 490-495.

- [7] Pannetrat, A., and Molva, R. 2003. Efficient Multicast Packet Authentication, *Proc. 10th Ann. Network and Distributed System Security Symp. (NDSS '03).*
- [8] Rivest, R.L., Shamir, A., and Adleman, L. 1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. ACM*: 120-126.
- [9] Harn, L. 1998. Batch Verifying Multiple RSA Digital Signatures, *IEE Electronic Letters*: 1219-1220.
- [10] FIPS PUB 186. 1994. Digital Signature Standard (DSS).
- [11] Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M., and Pinkas, B. 1999. Multicast Security: A Taxonomy and Some Efficient Constructions, *Proc. IEEE INFOCOM*: 708-716.
- [12] Perrig, A., Canetti, R., Song, D., and Tygar, J. 2001. Efficient and Secure Source Authentication for Multicast, *Proc. Network and Distributed System Security Symp. (NDSS '01).*
- [13] Merkle, R. 1980. Protocols for Public Key Cryptosystems, *Proc. IEEE Symp. Security and Privacy*.
- [14] Zhou, Y., Zhu., X and Fang, Y. 2010. MABS: Multicast authentication based on batch Signature, *IEEE Trans. Mobile Computing*: 982-993.
- [15] Hui, C.X., Zhi, D.J. 2010. Design of SHA-1 algorithm based om FPGA, Proc. International Conference on Networks Security, Wireless Communications and Trusted Computing.
- [16] Harold, E.R. 2004. Java Network Programming, Third edition, O'Reilly publications.
- [17] Harte, L. 2008. Introduction to Data Multicasting, Althos publications.
- [18] Jaworski, J., and Perrone, P. 2000. Java Security Handbook, Sams Publications.
- [19] Paar, C., Pelzl, J. 2009. Understanding Cryptography, Springer publications.
- [20] Stallings, W. 2005. Cryptography and Network Security Principles and Practices, Fourth edition, Prentice hall publications.
- [21] Pitt, E. 2006. Fundamental Networking in Java , Springer publications.