Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Enhancement of VoIP Protocols using ECC

Gautam Bommagani*
Tata Consultancy Services
Hyderabad, India

Apoorva Paidipelli
Hyderabad JNTU
Hyderabad, India

Vinit Kumar Gunjan
BioAxis DNA Research Centre (P) Ltd
India

Pooja Singh
Dot Spiders Info Solutions (P) Ltd
India

Abstract: This paper explores the known VoIP related vulnerabilities and suggests solution to various security issues. This paper tries to reduce the gap between the vulnerabilities, detection and solutions to VoIP security issues. Understanding this gap will help to identify what issues need to be addressed in the future development of VoIP applications? This paper provides a solution to denial of service attacks through network modeling and a solution to man in middle attacks using Elliptic Curve Encryption. The use of ECC proposed in various papers is limited to key exchange and authentication algorithms, not encryption. This paper also provides an approach to convert a plain text message in to elliptic curve points, which can further be used to implement Elliptic Curve Encryption/Decryption algorithms.

Keywords: Simple mail transfer protocol (SMTP), ECC, RSA, User Agent Client(UAC)

1. Introduction

VoIP refers to the transmission of datagram packets over the IP network, commonly known as Voice over Internet Protocol. Because of the efficiency that the IP network provides, VoIP is becoming very popular. And popular applications and devices tend to become popular targets for the attackers. Since the majority of public will soon rely on the VoIP and wide spread attacks could be devastating and significantly impact commerce and public safety. Since people have become accustomed to the high availability of PSTN[1], so are likely to expect VoIP to meet that service level.

Many companies and open source groups have already begun tailoring security programs such as vulnerability assessment tools, intrusion detection systems and firewalls etc. However there is no proof that these tools operate as thoroughly as they are required. This paper examines the functionality current VoIP security to determine their limitations. The paper also demonstrates how to handle the problems of Denial of Service attacks, using network modeling. Since the audio information that travels over internet during any session in VoIP is in plain format, it can be intercepted by any hacker to steal confidential information. The papers [1,2,3] referred for ECC are all meant for key Exchange and Authentication. None of them has proposed ECC as an encryption algorithm to encrypt the audio information that travels over the internet. This paper provides an approach for the implementation of ECC encryption for audio signals. Because of its small size and low processing elliptic curve encryption algorithms provides efficient, more reliable and more secure communication. The paper is divided into different sections as follows. Section 1 is the brief introduction of the VoIP protocols and the applications. It also provides the brief introduction of various proposed algorithms and mechanisms for the security improvements in the VoIP applications. Various reasons that are responsible for making Voice communication vulnerable in the hostile environment of Internet are discussed in section 2. In section 3 and 4, one of the most popular VoIP protocol, Session Initiation Protocol, is discussed to depict the point of vulnerabilities and various commonly occurring attacks. The solutions these vulnerabilities is presented in section 5. One of them is the mechanism for tackling the Distributed Denial of service attacks. Second is the proposal of Elliptic Curve Cryptography for the encryption of audio stream in the voice of internet protocols. The section also provides a mechanism for the implementation of conversion of plain text into elliptic curve point, which can facilitate the ECC encryption/decryption in real time applications. The results are discussed in section 6 and a comparison between ECC and RSA

2. Vulnerabilities

The vulnerabilities encompass not only flaws inherent within VoIP application itself but also in the underline operating systems, application and protocols that VoIP depends upon. This section focuses on the threats that can cause even more concern when we think that VoIP is in fact replacing the oldest and most secure communication system that world has ever known, that is PSTN network. Once a vulnerability has been identified and validated it can be can be used later for

larger attacks. It is the combination of vulnerabilities that allows the attacker to reach through many different networks and traverse all these networks unnoticed and launch large attacks on unsuspecting networks. The paper considers SIP as standard protocol for analyzing the various vulnerabilities in the VoIP network. Thus the paper mainly focuses on the SIP security issues and proposes solutions to them.

3. Session Initiation Protocol

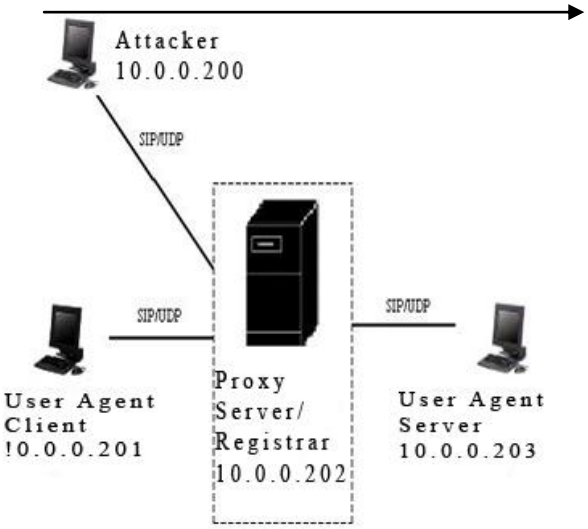
The SIP [4] protocol is derived from the Simple mail transfer protocol (SMTP) and Hyper Text Transfer Protocol (HTTP). SIP was designed to provide following important capabilities:

a. Location of participant in the Session
b. Participant availability
c. Participant Capability
d. Session setup
e. Session Management

SIP derives its authentication mechanism from HTTP, it uses the basic and digest schemes for authentication. In basic scheme the client provides a user ID and password sent in clear text, which is clear vulnerability. In the digest scheme password is encrypted in MD5 algorithm. However this mechanism is also compromised if relay attacks is used. The basic working of SIP between a User Agent Client [4] (UAC) and User Agent Server [4] (UAS) is given by:

The response codes used by SIP are same as that used by HTTP. Since internet is the foundational service used by Voice over IP, and the internet itself can be considered as a hostile environment for security point of view. All internet users must protect their transmissions from potential attackers, and SIP users are no exception. This is true for both security of SIP enabled sessions and also for SIP signaling security.

Authentication [1,2] is a security feature that ensures that access is given only to the users who are permitted to access. In SIP based network authentication can take place between the user agent and the server, where server requires a user agent to authenticate itself before processing request. Similarly a user agent can request the authentication of a server (known as Mutual Authentication). However during call involving user agent and server, an attacker could masquerade a user, forging the real identity of the sender. The basic attack model between user agents and server is given as follows:



4. Security Threats and Attacks

This section presents some threats that could be used to exploit the VoIP network. These attacks have been discussed in [4,5,6] papers. These attacks show the vulnerabilities at various levels of Voice over Internet Protocols. In this paper we have discussed these vulnerabilities in order to propose solutions to them. The attacks related to flash crowds, Denial of Service and Distributed denial of service has been referred from paper [7,8]. This section also illustrates the points of vulnerabilities that encourage various attacks. Threats and attacks to breach the lower level encryption protection (E.g. TLS and IPSec) are not discussed in this paper. The most common methods that are used while attacking a VoIP network are:

- Replay attacks

Replay attack involves a malicious user retransmitting a genuine message in order to establish authorized communication with the entity receiving the message. Replay attack is a common threat to client-server systems that use messages as communication means.

- Registration Hijacking

Registration hijacking is a sort of replay attack conducted during registration process. If an attacker can capture the legitimate register message, then modify and send a new register message to the registrar within the period set in the original time stamp, he can fool the registrar in many ways. For example the attacker can de-register the existing

registration by modifying the Expires header field with the value 0. In this case the original registrant cannot send or receive calls; and cannot register his or her own device as appropriate contact address, there by redirecting all requests for the affected user to the attacker's device.

- Session tear down

This attack is used to *tear down* a normal conversation session between legitimate users by sending a bye message to either user. To launch this attack the attacker has to somehow learn the parameters of the previous call control request, then build his own bye message. Vulnerability of this type of attack is caused by lack of authentication mechanism for Bye request in the SIP standard.

- Tempering message bodies

Since SIP messages are forwarded in clear text, it is not necessary for someone to have a decoder. Simply capturing messages is good enough. Once a hacker has captured a message, the message body and the headers in the SIP message can be modified. A hacker may capture an "invite" message from a subscriber and change from header to reflect his or her own address. Tempering of messages can be prevented by using encryption, therefore hacker would not be able to change it and route it back to the network.

- Denial of service and Amplification

In this type of attack, the hacker just floods the network with specific type of traffic. By launching the flood of requests to an application server, the network element is immediately flooded and congested, taking it out of service. Now when redirect services are used the potential for amplifications occur. One message is forked into many different messages, which will result in many different responses. Thus the unwanted requests are multiplied and send to many destinations. A similar kind of attack towards registrar involves many different identities. Each identity consumes memory within the registrar and therefore if a large number of registrations take place, in the registrar runs out of memory and hence will not be able to serve anymore.

- Bots and DDoS Attacks

Bots are simple scripts that are carried to a subscriber's device through websites and other viruses transported using text messages or email. Now a bot [7,8] sits on the device and looks for open ports or connections that can be used to access the internet. It then looks for other systems or devices on the network and start exploiting them. This leads to self propagation of the bots on the network. The most troublesome aspect of a bot is the ability to control the script from remote server using IRC protocol. They receive the commands from the server connected to the URL that basically launches the script. The server becomes the command and control center. When these bots spread over a small network they from a botnet, which can be used for *DDoS [7,8]* attacks. Imagine if cell phones were infected with these bots. The hacker would then have millions of cell phones at his/her disposal. Now if all these cell phones placed a call to same destination, that portion of network would be out of service for an undetermined amount of time.

- Rouge Sets Attacks

Rouge [7] sets attack refers to deceive for the purpose of gaining access to someone else resources. The intruders perform digital impersonation by adding a new set of VoIP applications to attacked IP networks, when spoofing an identity of a targeted call participant. Then the malicious VoIP application can conduct any activities that may harm the attacked IP network. A lockdown mechanism can be used as a counter measure. Only administrators can add new set of VoIP applications to the network, with administrator password and logs are sent to the network and administrator. Also the application must also reject any more entries if more than three passwords are attempted.

5. Proposed Solutions to the various Attacks

SIP suffers from all the above mentioned attacks. Since SIP is based on HTTP and SMTP protocols [4], so it suffers from the same security issues and attacks as these protocols. Since the SIP packets are transferred using RTP [9] protocol for transferring media. The RTP protocol is also based on UDP protocol, the media stream can be intercepted by any hacker and can easily be decoded. This will ultimately leads to information leakage.

The authentication mechanism can be used to provide security from registration hijacking but authentication alone cannot provide complete security. The data stream needs to be encrypted using an encryption algorithm like PGP, GPG, ECC or ZRTP protocols that use hash functions to generate encrypted algorithms. These algorithms should be fast enough, so that the efficiency and quality of service is not compromised. The security measures for attacks like DDoS [7,8] and Flash crowds [7,8] also need to developed so that the performance of protocol never goes down due to unwanted traffic. The various mechanisms like push-back mechanisms [11,13] can be used to throttle the traffic at the routers that are routing traffic. We also need to develop algorithms like Fair Queuing Algorithm [11,13] that can classify which type of traffic is responsible for the congestion[11], because congestion can also be due to genuine load. So need an algorithm that can classify the aggregate traffic that is causing the congestion. Next we need a mechanism which could take counter measures to control mechanism. Instead of throttling traffic at just one router we can throttle it at various routers, which ultimately decrease the load on a single router and will increase the performance. A protocol should be developed that can communicate with the upstream routers to provide them the information about the unwanted traffic or the traffic that is causing Network slowdown.

- **Counter measure for DDoS Attacks**

Sine this attacks is not based on the vulnerability in the SIP implementation, so it cannot be tackled by making any improvements in SIP protocol. To tackle this attack we need to use a mechanism at the routers that can detect this attack

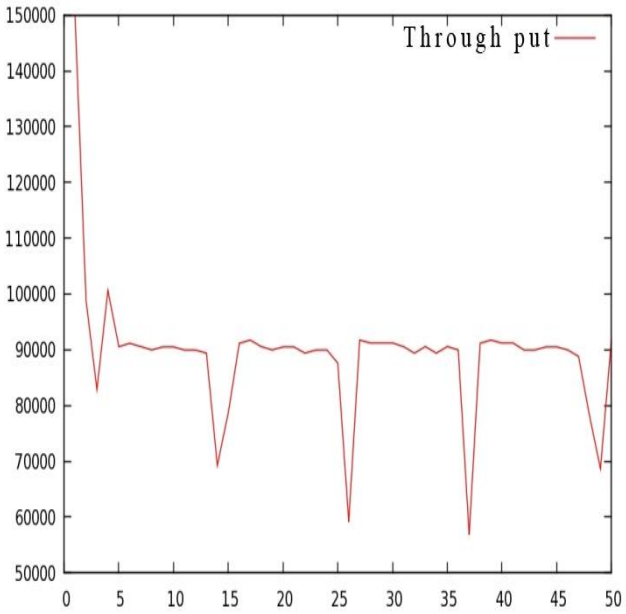
and take counter measures. NS-2, an open source network simulator is being used to simulate this mechanism. The two mechanisms simulated for security enhancement of Voice over Internet protocol VoIP are:

a. *DropTail*: Most generally used queuing mechanism in the router also uses jacobsons algorithm when queue fills up. There is a common queue for both TCP and UDP packets when the queue fills up according to jacobsons algorithm the TCP window size is reduced to its minimum threshold value since TCP packets can be retransmitted so the quality of service do not suffer to much but in case of UDP the dropped packets cannot be retransmitted. UDP packets suffer from congestion and quality of service suffers.

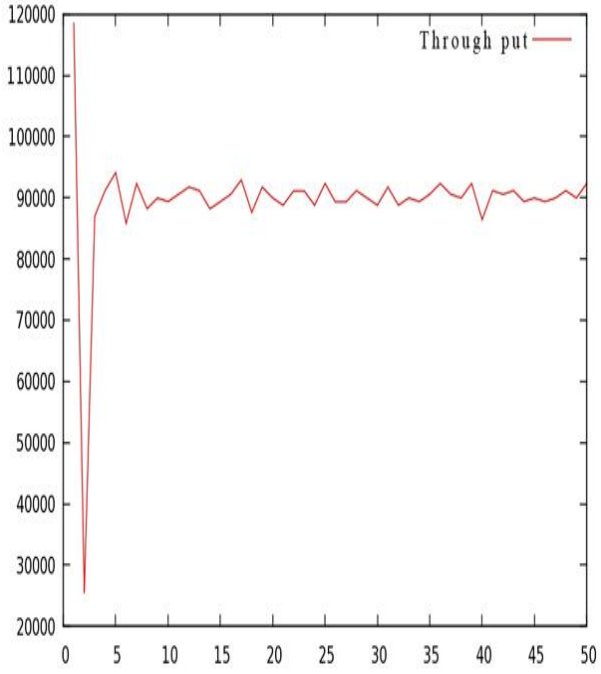
b. *Random early discard (RED):* In this mechanism we divide the queue for TCP and UDP. There is a minimum and maximum threshold value within which TCP packets can be queued and the left out queue size is used for UDP packets. The probability of next incoming TCP packet dropped depends on the average number of packets currently in the queue. The probability of dropping next incoming packet is equal to ratio of average to the maximum threshold value. So when average is equal to maximum threshold value the next incoming packets are dropped. Since UDP has a separate queue so it suffers less as compare to droptail mechanism.

The results generated from the simulation are as follows:

a. Graph for DropTail mechanism:



b. Graph for Random Early Discard mechanism:



It is clear and can be inferred from the above graphs that Drop tail provides much consistent traffic and has a separate window for UDP traffic. Furthermore a fair queuing algorithm can be used to classify the type of packets that are responsible for the attacks, and this information can be transmitted to the routers that are above the algorithm invoking router, so that traffic can be controlled router by router, which will be capable of tackling much bigger DDoS [11,13] attacks.

- **ECC encryption for messages**

Since the media stream is send in UDP datagram packets, any attacker can intercept these packets, which will lead to information leakage. The attacker can also temper this stream to send his/her message. So there is a need of a encryption algorithm that can be used for the encryption of the media stream. But since the VoIP is a real time application and Internet was not designed to support real time application, hence we cannot afford delays and losses. Now the encryptions standards like RSA that are supposed to provide the best encryption are too slow to be used in VoIP applications. So there is a need to develop a encryption algorithm that provides the same security that RSA provides but at much less cheaper price in terms of computation time. ECC [1,2,3] (Elliptic curve cryptography) is an algorithm which uses the elliptic curves for the encryption and have much smaller encryption keys as compared to RSA. 192-bit ECC key encryption provides the same security that a 1024-bit RSA key encryption can provide.

- **RSA Algorithm**

RSA algorithm is based on the fact that, it is easy to multiply two numbers with a computer but it is very difficult to factor two numbers. For example, if I ask you to multiply together 34537 and 99991, it is a simple matter to punch those numbers into a calculator and 3453389167. But the reverse problem is much harder.

RSA Key Generation

1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
2. Compute n = pq and (φ) phi = (p-1)(q-1).
3. Choose an integer *e*, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent *d*, 1 < d < phi, such that ed ≡ 1 (mod phi).
5. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

- n is known as the *modulus*.
- e is known as the *public exponent* or *encryption exponent* or just the *exponent*.
- d is known as the *secret exponent* or *decryption exponent*.

RSA Encryption:

Sender A does the following:-

1. Obtains the recipient B's public key (n, e).
2. Represents the plaintext message as a positive integer *m*
3. Computes the ciphertext $c = m^e \bmod n$.
4. Sends the ciphertext *c* to B.

RSA Decryption

Recipient B does the following:-

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.
2. Extracts the plaintext from the message representative *m*.

When we talk about the *key length* of an RSA key, we are referring to the length of the modulus, *n*, in bits. The minimum recommended key length for a secure RSA transmission is currently 1024 bits. A key length of 512 bits is now no longer considered secure. The longer your information is needed to be kept secure, the longer the key you should use.

- **ECC Algorithm**

The paper proposes Elliptic curves over the finite field GF(2^m)[3]. The finite field GF(2^m) consists of 2^m elements, together with the addition and multiplication operations that can be defined over the polynomials. Thus m is the order of the reduction polynomial being used. For elliptic curves over GF(2^m), a cubic equation is used in which the variables and coefficients all take on the values in GF(2^m). The general form of the equation is

$$y^2+xy = x^3+ax^2+b$$

where x, y, a and b are the elements of GF(2^m). In elliptic curves point O represents a point at infinity. Now if P and Q are any points on elliptic curve, then the addition of P and Q is defined as

$$P+Q = R$$

where R is point of intersection of the line drawn between P and Q. Thus

$$P+O = P$$

If P=(xp,yp) and Q=(xq,yq) with P! = Q and

P! = -Q then R = P+Q = (xr,yr) is determined by the following rules:

$$xr = \mu^2+\mu+xp+xq+a$$
$$yr=\mu(xp+xr)+xr+yp$$

where

$$\mu=(yp+yq)/(xp+xq)$$

For multiplication say 2P we just need to add P to itself. That is if

$$R = 2P = (xr,yr)$$

Then

$xr = \mu^2+\mu+a$

$yr=xp^2+(\mu+1)xr$

where

$\mu = xp+(yp/xp)$

To implement the Elliptic curve cryptosystem in VoIP application we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete logarithm. In implementation we take any point (say Q) on the elliptic curve which will serve as a base point. Now we need to calculate a factor k(very large) such that

$kQ = O$

This is a discrete logarithmic problem, because even if kQ=P, it is relatively easy to calculate P given k and Q but it is hard to determine k given Q and P. Now for kQ=O, k serves as the factor which will find a point at which, if a tangent is drawn then it will intersect the curve at infinity.

Now a user (say A) can select any number say na such that

$na < k$

This na serves as a private key for the user. Now to generate a public key the user A will compute his public key Pa as

$Pa = na * Q$

Similarly user B can also generate his private key (nb) and public key Pb. Now for exchanging keys Diffie-Hellman Key Exchange Algorithm can be used. Now upon receiving B's public key A will generate a shared key (say K) as

$K = na * Pb = na * nb * Q$

Similarly B will generate the shared key as

$K = nb * Pa = nb * na * Q$

Now if we examine both the equation then it is clear that both equations will produce same results. Now since we have send public keys over the internet, so even if they are compromised the attacker will not be able to decipher the message because the actual key used for encryption is a shared key that was never transferred over the network.

- Elliptic Curve Encryption

For the elliptic curve encryption [3] the first task is to convert the plain text message in to the points on the elliptic curve, which is more difficult than just encryption. This paper provides following approach to convert plain text into a point:

Take the value of the plain text as X coordinate and compute the Y coordinate. This will give two values of Y (-ve and +ve). So in order to have coherence for encryption and decryption the two communicating parties have to agree upon one of the values. After converting the plain text in to the point say Pm we can use it for ECC encryption

Now if Q is the base point being used by the two parties (A and B), the sender of the message (say A) will choose a random variable k and produces the ciphertext Cm consisting of pair of points

$Cm=\{kQ,Pm+kPb\}$

where Pb is B's public key that A is having.

- Elliptic Curve decryption

To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point.

$Pm+kPb-nb(kQ) = Pm+k(nb*Q)-nb(kQ) = Pm$

A has masked the message Pm by adding kPb to it. Nobody but A knows the value of k, so even one knows the public key Pb, nobody can remove the mask kPb. However A also includes a clue, which is enough to remove the mask if one B's private key is known.

Thus ECC provides the message exchanges using points which are of no use if intercepted by any attacker, because it is not possible to guess the elliptic curve from the points. Being small in size the ECC provides faster encryption with equal security as RSA provides. Thus maintaining the quality of service.

6. Conclusions

In this paper we presented the common threats for VoIP security and the problems that a Voice over Internet Protocol suffers from. We simulated Denial of service attacks using NS (network simulator tool). We also proposed solution to Denial of service attacks by using Random Early discard, fair queuing algorithms. The simulation for security measures against Denial of service attacks give positive results as expected. In the next step we proposed ECC as encryption algorithm for the media stream in the SIP protocol. ECC provides the same security that RSA can provide with 1024 bit encryption at much cheaper rate in terms of key size. This reduces the computation overhead and hence the quality of service of VoIP is not compromised.

References

[1] Wu , L., Zhang, Y., Wang, F.,(2009), "A new provably secure authentication and Key agreement protocol for SIP using ECC ", *Computer Standards and Interfaces*, vol. 31, pp-286-291.

[2] Aydos, M., Sunar, B., Koc, C.K., "An elliptic curve based authentication and key agreement protocols for Wireless Communication", *Electrical and computer Engineering. Oregon state university Corvallis, Oregon 97331*

[3] William Stalling, (2006)"*Cryptography and network security*"4th edition, Prentice Hall.

[4] Russel,T., (2008), "*Session Initiation Protocol (sip) Controlling Convergent Networks*"McGrawHill Professional.

[5] Seedorf, J., (2006), "SIP Security: Status Quo and Future Issues"**,** *Talk presented at 23rd Chaos Communication Congress.*

[6] Qiu, P.Q., Monkewich,O., and Probert,R.L., (2004), "SIP Vulnerabilities Testing in Session Establishment and User Registration" *ICETE (*2), 223-229

[7] Hung, P.C.K., Martin, M.V., (2006) "Security Issues in VoIP Applications". *In proceedings of Canadian conference on Electrical and Computer Engineering, CCECE'06* , pp-2361-2364

[8] Hung, P.C.K., Martin, M.V., (2006) "Through the Looking Glass: Security Issues in VoIP Applications". *In proceedings of Canadian conference on Electrical and Computer Engineering, CCECE'06* ,

[9] Sawda, S., Sawda,R , Urien, P., Ibrahim Hajjeh, I. (2008) "Non Repudiation for Session Initiation Protocol", *Information and Communication Technologies: From theory to Applications, ICTTA 2008,* 7-11 April 2008, pp- 1-5.

[10] Gupta, P., Shmatikov,V.,(2007) "Security analysis of Voice over IP protocols" *Proceedings of the 20th IEEE Computer Security foundation Symposium –CSF-07,* pp- 49-63.

[11] Demers, A., Keshav, S., and Shenker, S.,(1989). "Analysis and simulation of a fair queuing algorithm", *SIGCOMM Symposium Proceedings on Communications , architectures and protocols* , pp-1-12

[12] Dhamankar, R.,(2004) "Intrusion Prevention: The Future of VoIP Security", *Tipping Point Technologies*, Retrieved from http://www.tippingpoint.com/

[13] Mahajan, R., Bellovin,S.M., Floyd, S., Joannidis, J.,Paxson, V., and Shenker, S., "Controlling high-bandwidth aggregates in the network," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 3, pp. 62-73, 2002.

