RSA algorithm: first, it is very expensive to compute. And second, the memory overhead is large. So, Elliptic Curve Digital Signature Algorithm (ECDSA) is used for digital signing [2]. The elliptic curve analogue of the Digital Signature Algorithm (DSA) is the Elliptic Curve Digital Signature Algorithm (ECDSA).

3.3.2 ECDSA algorithm

The prime reason for the popularity of ECDSA [2] algorithm is that, there is no sub exponential algorithm have been developed to solve the elliptic curve discrete logarithm problem on specifically chosen elliptic curve. Hence, ECDSA takes the full exponential time to solve the problem, while other best algorithm developed for solving the fundamental integer factorization for RSA and discrete logarithm problem in DSA; both of them take sub exponential time. A highly secured key is generated by the implementation. And as small key size is used in the elliptic curve, thus it consumes lesser bandwidth.

As compared to competitive systems like, RSA and DSA, ECDSA uses significantly smaller parameters, but with the security of equivalent level [8]. Having smaller key has some benefits, which includes faster computation time and reduction in storage space, processing power and bandwidth as well. Due to this features, ECDSA is ideal for constrained environments like pagers, PDAs, smart cards and cellular phones.

4. Comparison Parameters

Base on some parameters, comparison of processing modes PPM, DPM and DFM is summarized in following Table 1.

Table1: Comparison of IP Traceback Approaches.

Parameters	*PPM*	*DPM*	*DFM*
Computational Overhead	Moderate	Low	Very Low
Maximum Traceback Ability	Edge Router	Upto ingress interface of edge router	Upto attacker node
Flow Marking	No	No	Yes
No. of packets marked at ingress interface of edge router	Random number of packets	Each packet of every flow	Few packets of every flow
Minimum Packets required to Trace IP	More than DPM	More than DFM	Minimum 4

5. Conclusion and Future Work

With increasing number of internet users, issue of tracing the source of Denial of Service (DoS) attack is reviewed. In this paper, a wide survey has been carried out to identify and classify the existing IP traceback schemes. Selecting the best method for packet marking is the key point in tracing the source IP. Challenges of previous IP traceback methods was, reconstructing the attack path efficiently and tracing exact attacker node hidden by a NAT or proxy server. These challenges are overcome by DFM IP traceback approach. In addition it provides optional authentication method. DFM provides higher traceback accuracy and authentication, but victim resources in attach path are consumed even before the traceback is completed. Therefore, a need arises to provide a mechanism to preserve the resources in attach path even before the IP traceback. To accomplish this, attack detection, prevention and traceback with novel approch can reinforce complete security platform to preserve the resources in attack path even before traceback..

References

[1] Ansari, Belenky, N. “Deterministic Packet Marking”, New Jersey Institute of Technology, 2005.
[2] Aqeel Khalique, Kuldip Singh, Sandeep Sood, “Implementation of Elliptic Curve Digital Signature Algorithm”, Indian Institute of Technology, Roorkee, 2010.
[3] A. Yaar, A. Perrig, D. Song, “Pi: A Path Identification Mechanism to Defend Against DDOS Attacks” Proc. Symposium on Security and Privacy, 2003.
[4] B. Gong., K. Sarac, “IP Traceback based on Packet Marking and Packet Logging”, University of Texas at Dallas, 2005.
[5] D. X. Song, A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” INFOCOM, 2001.
[6] D. Johnson, A. Menezes and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Certicom Corporation, 2009.
[7] M. T. Goodrich, “Efficient Packet Marking for Large-Scale IP Trace back,” Proc. Ninth ACM Conference of Computer and Communication Security, 2002.
[8] National Security Agency/ Central Security Service (NSA/CSS), the Case for Elliptic Curve Cryptography.
[9] R. Shokri, A. Varshovi, H. Mohammadi, N. Yazdani, B. Sadeghian, “DDPM: Dynamic Deterministic Packet Marking for IP Traceback”, 2006.
[10] S. K. Rayanchu, G. Barua, “Tracing Attackers with Deterministic Edge Router Marking”, 2005.
[11] S. Matsuda et al., “Design and Implementation of Unauthorized Access Tracing System,” SAINT 2002.
[12] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Network Support for IP Traceback,” IEEE/ACM Transactions on Networking, 2001.
[13] T. Subbulakshmi, I. A. A. Guru and S. M. Shalinie, “Attack Source Identification at Router Level in Real Time using marking Algorithm Deployed in Programmable Routers”, ICRTIT, 2011.
[14] V. Aghaei-Foroushani and N. Zincir-Heywood, “Deterministic and Authenticated Flow Marking for IP Traceback”, The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013), March 2013.
[15] V. Kuznetsov, H. SandStrom, A, Simkin, “An Evaluation of Different IP traceback Approaches”, Information and Communications technology, 2002.
[16] Y. Tseng, H. Chen and W. Hsieh, “Probabilistic Packet Marking with Non-Preemptive Compensation,” IEEE Communications Letters, vol. 8, no. 6, pp. 359–361, JUN 2004.
[17] Z. Gao, N. Ansari, “Tracing Cyber Attacks from the Practical Perspective”, IEEE Communications Magazine, 2005.