Schemes Involved in Pollution Attacks in Network Coding- A Survey

Sangeetha.V[1], Radhapriya.S[2]
1M.Phil Scholar, Government Arts College, Coimbatore.
2Assistant Professor of Computer Science
Government Arts College, Coimbatore.

Abstract
Security is the important issue in all the networking areas. In this paper we surveyed several schemes working with Pollution Attacks in Network Coding. Network coding in different approaches is used to characterize the region for multicast networks and it also used to encode the received packets. Network coding is a common technique which is used to improve the System's throughput, efficiency and reliability. Network coding is mainly classified into two forms. Inter-session and Intra –session network coding.

Index Terms— Homomorphic Signatures, MAC Schemes, Network Coding, Pollution Attacks.

1.Introduction

Network coding framework deals with random packet loss, change of topology and delays. Network coding is used to improve the throughput for multicast and even unicast transmissions [1], [2], [3]. The main idea of this approach is the server breaks the file into smaller blocks and send it to the system whenever the system needs it. The network coding system is used to protect the system against malicious nodes. It allows the users to mix the information content in packets before forwarding them to the nodes. Mixing of information can be done in a distributed manner.

Pollution attacks are also called as Jamming [4] [5] and Byzantine attacks [6]. Pollution attacks in intra-session coding have received significantly less attention [7], [8]. There are so many pollution attack related problems involved in network coding technique.

During the decoding process all the packets are decoded wrongly. The whole network will get affected quickly or get polluted. Pollution attacks are always initiated in a single packet transmission.

2.Schemes Involved in Pollution Attacks

In Network Coding there are several schemes involved in Pollution Attacks. The schemes are i) Homomorphic Schemes ii) homomorphic MAC Schemes iii) Hash Functions iv) Homomorphic Signatures.

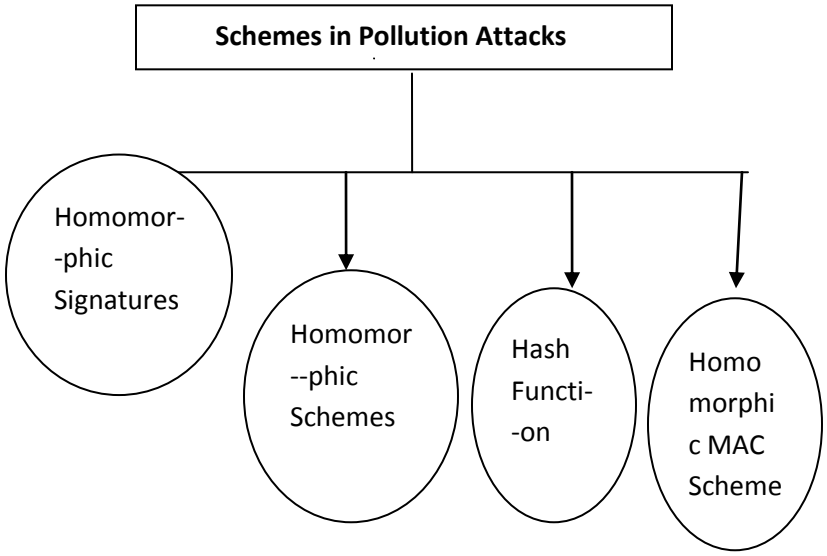

Figure 1. Schemes involved

2.1.Homomorphic Signatures

In Homomorphic Signature schemes 3 different schemes are used.

I) Hash Scheme
II) Inter MAC_{CPK}
III) Space MAC_{pm}

Network coding is defined as a Probabilistic – Polynomial, Time- algorithmic (i.e) Setup, sign, Combine & verify. Homomorphic Signature Scheme is used to provide the inner-network detection for

Network Coding. Homomorphic Signature are gathered from Multiple Source that is defined in 4 algorithms i) Generated algorithm ii) Sign algorithm iii) Combine algorithm and iv) Verify algorithm.

The signature scheme proposed in [9] uses a standard signature scheme that based upon the hardness of discrete logarithm problem. The blocks of data are considered as vectors spanning a subspace. The signature is not calculated for every data blocks, but for vectors subspace. The signature verification allows to check if the received vector belongs to the data subspace and the file is authenticated. This scheme also requires fresh keys for every file.

The signature schemes proposed in [9] follow the approach used in improvements in terms of public key size and per packet overhead. The signature schemes proposed are designed to authenticate a linear subspace designed by the vectors containing data blocks. Signatures on a linear subspace are more than enough to authenticate all the vectors used in this same subspace. With these schemes, a single public key can be used to verify multiple files By comparing the different scheme's proposed in [9] provides the security to data transmission in the network and minimizes the pollution in the network.

Zhao et al. [9] proposed a non-homomorphic signature scheme that used subspace checking to verify the packet. But their scheme requires the source to know the whole file before the transmission.

Boneh et al. generalized the scheme to support data streaming by involving public key signatures for each individual vector. Compared with digital signature schemes, message authentication codes (MACs) are used against pollution attacks. However, the corrupted packet may not be identified at the first hop downstream node and thus it may pollute other packets. In MAC it suffers tag pollution attacks.

2.2.Homomorphic MAC Schemes

MAC is used for expanding spaces and are called $Space_{MAC}$. This is allowed a node to verify the received packets. MAC algorithms are sometimes called as HASH keypad function. MAC's output's are sometimes called as tag. MACs differ from digital signatures. The term Message Integrity Code (MIC) is frequently substituted for the term MAC.

MAC algorithms can be constructed from other cryptographic primitives, such as However many of the fastest MAC algorithms such as UMAC and VMAC are constructed based on universal hashing

2.3.Homomorphic Schemes

Homomorphic Functions can be used with Network Coding to verify the blocks are received at each Single system [10], [11], [12].

2.4.HASH Functions

Existing mechanisms implementing homomorphic hashes or homomorphic signatures are computationally expensive. The mechanisms that implements message authentication codes (MACs) are also suffering from some problems like large number of colluding peers, works on fixed acyclic graph networks.

Definition 1: Hash function H is one-way if, for random key k and an n-bit string w, it is hard for the attacker presented with k,w to find x so that Hk(x) = w. [13].

Definition 2: Hash function H is second-preimage resistant if it is hard for the attacker presented with a random key k and random string x to find y 6= x so that Hk(x) = Hk(y)[13].

Definition 3: Hash function H is collision resistant if it is hard for the attacker presented with a random key k to find x and y 6= x so that Hk(x) = Hk(y) [13].

Generic attack is a common attack that is seen in all Hash functions. A hash function is used to cut the actual string into specific length. Hash function is used to provide data integrity and to make a digital signing more efficient. Commonly Crypto Hash functions have the following properties:

- preimage resistant
- weak collision resistant
- strong collision resistant

Three main types of Hash Functions are MD5, RIPEMD-160 and SHA-1. The MD5 outputs

digests of 128 bits, while RIPEMD-160 and SHA-1 produce digests with 160 bits.

3.Conclusion

In this paper we have surveyed several schemes involved in Pollution Attacks in Network Coding. There are still several schemes involved in the network coding areas. We just focused on the Homomorphic Schemes, Homomorphic MAC Schemes, Hash Functions and Homomorphic Signatures.

REFERENCES

1.T. Ho, M. M´edard, M. Effros, and D. Karger, "The benefits of coding over routing in a randomized setting," in Proc. IEEE Symposium on Information Theory (ISIT'03), Kanagawa, Japan, July 2003.

2.Z. Li and B. Li, "Network coding: the case of multiple unicast sessions," in Proc. 42th Annual Allerton Conference on Communication, Control, and Computing, September-October, 2004

3. D. S. Lun, M. M´edard, and R. Koetter, "Network coding for efficient wireless unicast," in Proc. 2006 International Zurich Seminar on Communications (IZS'06), Zurich, Switzerland, February 2006.

4. C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in Proc. of IEEE International Conference on Computer Communications (INFOCOM), 2006, pp. 1–13.

5. E. Kehdi and B. Li, "Null keys:limiting malicious attacks via null space properties of network coding," in Proc. of IEEE International Conference on Computer Communications (INFOCOM), 2009, pp. 1224–1232.

6. F. Zhao, T. Kalker, M. Medard, and K. J. Han, "Signatures for content distribution with network coding," in Proc. of IEEE International Symposium on Information Theory (ISIT), 2007, pp. 24–29.

7. S. Agrawal, D. Boneh, X. Boyen, and D. Freeman, "Preventing Pollution Attacks in Multi-Source Network Coding," in PKC'10, 2010.

8. J. Dong, R. Curtmola, C. Nita-Rotaru, and D. Yau, "Pollution Attacks and Defenses in Wireless Inter-flow Network Coding Systems," in WiNC'10, 2010.

9. D. Boneh, D. Freeman, J. Katz, and B. Waters," Signing a Linear Subspace: Signature Schemes for Network Coding". Springer, Mar. 2009.

10. D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in Info Sciences and Systems, vol. 1, no. 1, 2006.

11. Y. Zhu, B. Li, J. Guo, "Multicast with network coding in application layer overlay networks", IEEE JSAC on Rencent Advances in Service Overlay Networks, Vol. 22, no. 1, pp. 107- 120, Jan. 2004.

12. D. Petrovic, K. Ramchandran, and J. Rabaey, "Overcoming Untuned Radios in Wireless Networks with Network Coding", IEEE Trans. on Information Theory, vol. 52, no. 6, pp. 2649-2657, Jun. 2006.

13. Ilya Mironov, "Hash functions: Theory, attacks, and applications", November 14, 2005.

14. Fr´ed´erique Oggier and Hanane Fathi "An Authentication Code against Pollution Attacks in Network Coding", September 17, 2009.

15. Anh Le, Athina Markpoulou," On Detecting Pollution Attacks in Inter-Session Network Coding",August 1,2011.

16. Dr Siddaraju, Chitresha Mehta," Cooperative Defense against Pollution Attack in P2P System with Network Coding", May 5,2013.

17. Shweta Agrawal, and Dan Boneh," Homomorphic MACs: MAC-Based Integrity for Network coding",2009.

18. Junsheng Wang, Jin Wang, Yanqin Zhu and Kejie Lu," SNKC: An Efficient On-the-fly Pollution Detection Scheme for Content Distributionwith Linear Network Coding" May 2009.

19. LIU Guangjun1, 2, WANG Bin1," Secure Network Coding Against Intra/Inter-Generation Pollution Attacks",March 3,2013.

20. Fang Zhao, Ton Kalker, Muriel M´edard, and Keesook J. Han," Signatures for Content Distribution with Network Coding" March 2010.

21. Stefan Pfennig and Elke Franz," Secure Network Coding: Dependency of Efficiency on Network Topology"December 2009.

22. Anh Le, Athina Markopoulou," TESLA-Based Defense Against Pollution Attacks in P2P Systems with Network Coding"April 2011.

23. Yaping Li1, Hongyi Yao2," RIPPLE Authentication for Network Coding"September 2013.

24.Levente Buttya´ n, La´ szlo´ Czap, and Istva´n Vajda," Detection and Recovery from Pollution Attacks in Coding-Based Distributed Storage Schemes".December 2011.

BIOGRAPHIES

Sangeetha.v, received her M.Sc degree in Information Technology from Bharathiar University, Coimbatore in 2013. She is currently a M.Phil candidate of Bharathiar University. Her research interests are in Advanced Networking.

S.RadhaPriya is working as Assistant Professor of Computer Science in the Post Graduate and Research Department of Computer Science, Government Arts College (Autonomous), Coimbatore. She has completed her M.Phil . She has about 18 years of teaching experience .

