Batch Signature for Mixed Signals in Wireless Networks

Battula Sudheer Kumar[1] (M.Tech)
P. Anjaiah[2] M. Tech
C.V.S.R College of Engineering, JNTU
C.V.S.R College of Engineering, JNTU

Abstract
In wireless networks interference is considered has a major problem. So, in order to avoid the interference we use the technique called mixing signal (Network Coding). The problem here is there are vulnerable to possible malicious attacks. i.e., if any of the intruder knows the information of other signal in the mixed signal they can be decoded easily. In order to resolve this problem we are proposing a good secure network coding scheme batch signature for mixed signal. So with the above network coding scheme we are providing a security to the signal.

Keywords: Batch Signature, Pollution Attack, RSA, Network Coding.

1. Introduction

All Wireless networks have been designed using the wires network as the blueprint. The design abstracts the wireless channel as a point-to-point link, and graft wired network protocol onto the wireless environments. For Example, routing uses shortest path protocols, routers forward packets but don't modify the data, and reliability relies on retransmission. The design has worked well for wired networks, but less so for the unreliable and unpredictable wireless medium.

A main distinguishing feature of a wireless network compared with a wired network is its broadcast nature, in which the signal sent by a node will reach all its destination neighboring nodes [1]. The signal will collide, if a neighbor apart from the target node is receiving data from more than one node at the same moment then the required signal will get cracked, which results in communication crash. In conventional or traditional wireless networks, this crash of signals may cause communication failure if no division technique is adopted. This will corrupt the system performance, which include packet loss rate and energy effectiveness.

In order to avoid interference problem we use mixing of signals are also called as (Network Coding Technique).

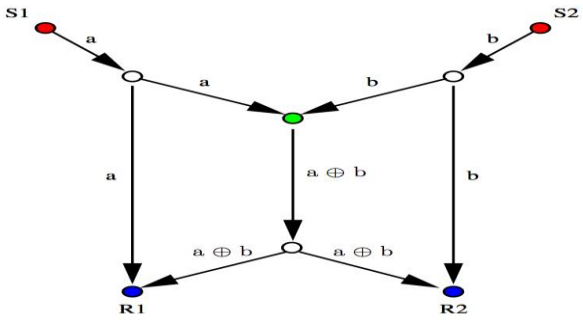

Fig: 1 Example of Network Coding

Network coding is described using the famous butterfly example [2]. Consider the network in Fig 2, where source S_i wants to deliver the signal a_i to both R_1 and R_2 and source S_2 wants to send the signal b_i to the same receivers. Assume all links have a capacity of one message per unit of time. If routers only forward the message they receive, the middle link will be a bottleneck, which for every time unit, can either deliver a_i to R_1 or b_i to R_2. In contrast if the router feeding the middle link XORs the two signals and sends a_i b_1 as shown in the figure, both receivers obtain two signals in every time unit. Thus, network coding allows the routers to mix the bits in forwards the mixed signal, as a single signal. At the receiver side we use signal recovery algorithm which will recover the useful signal from the mixed signal with already known information of the other signal and decrypt the signals thus the way we can get the original signal with out damaging the signal.

But the problem here is, if any intruder knows the information of other signal they can recover the original signal from mixed signal. So, In order to resolve this security issue we are proposing the Batch Signature for Mixed Signal. This scheme is based on the recently network coding technique which was first proposed by Ahlswede et al. [4] and Li et al. [5]. The rest of this paper explains about the Background, Batch signature overview, Limitations and Conclusion.

2. Background

The idea underlying batch signature in network coding is we can provide the security for the signal that is going to be recovered. In traditional mixed signal or network coding the intruder can decode the signal and get the useful signal easily if he knows the information of other signal [6]. To avoid this problem this paper proposes a scheme known as batch signature for mixed signal in wireless networks. A batch RSA digital signature scheme in which a signer can sign signals for multiple recipients simultaneously, with this scheme even if the intruders knows the information of other signal also he cannot decode the signal [7]. Batch RSA scheme will takes the three inputs to decrypt the original signal the first one is batch cipher text and second one is private key and third one is the information of other signal.

3. Batch Signature Overview

The network coding based applications are vulnerable to possible malicious pollution attacks. The batch signature [8] schemes have been well-recognized as the most effective approach to address this security issue. The pollution attack can be defined as that a malicious intermediate node can inject junk packets into the network to pollute the output, and further contaminate the entire downstream, preventing proper decoding. Formally, we describe the pollution attacks as follows. If any of the intruders as modified the signal or packet of the mixed signal then one invalid packet can destroy or corrupt the entire signal. So in order to provide the security we propose batch signature for network coding.

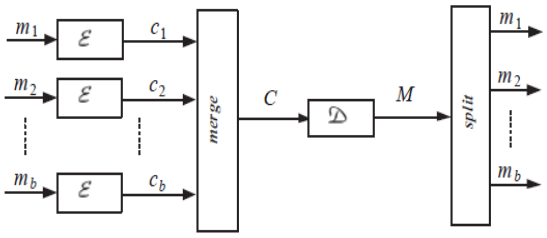

Fig: 2 Example of Batch Encryption & Decryption

Our scheme of wireless networks is shown in Fig. 2, where the source terminals $S_1, S_2 .. S_n$ intend to transmit signals $m_1, m_2 .. m_b$ to the receiver R1. In our scheme, at encryption side each signal is encrypted using public keys using RSA, after that each individual encrypted signal $c_1, c_2 .. c_b$ is going to mix(merge) and form a single signal called as encrypted mixed signal C, using the technique called network coding. At decryption side this encrypted mixed signal C, will received by the receiver and decrypt the signal using their private key and gets the mixed signal M and then decode the signals $m_1, m_2 .. m_b$ from the mixed signal using the signal recovery algorithm[9].

The Algorithm for batch cipher in Mixed Signals as follows

1. It takes a prime number as a security parameter to generate Public key and private key for encryption and decryption
2. Encrypt the each signal m1,m2..mn and sends the cipher signal to the reciever
3. Intermediate node takes the cipher text and merges as a single signal using a network coding techniwue and sends to the reciever.
4. At the receiver side decrypt the mixed signal (Cipher signal) .
5. Finally split the signal from the mixed signal using the signal recovey algorithm to get the actual signal.

4. Limitations

S.No	Security Strength
1.	Information Theoretic
2.	Equivalent to RSA
3.	Equal to the strength of crypto algorithm
4.	Not information theoretically secure but secure enough for the application
5.	Single point of failure

Table 1: Limitations of Scheme under Study

Ideally a good secure network coding scheme should consume less time and resources of the network, not be vulnerable, have ease of implementation and have good security strength.

5. Conclusion

In this paper, we have proposed an efficient security scheme for network coding against pollution attacks. The proposed scheme is using the Batch RSA for its signature with this secure communication is possible with out loss of rate. So, this scheme can achieve high efficiency and security in packet signature, and meet the important and emerging requirements for securing network coding.

6. References

Journals:

[1] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[2] J. Zhang, P. Fan, and K. B. Letaief, "Network coding for efficient multicast routing in wireless ad-hoc networks," IEEE Trans. Commun., vol. 56, no. 4, pp. 598–607, Apr. 2008.

[3] D. Charles, K. Jain, and K. Lauter, "Signatures for Network Coding," Proc. 40th Annual Conf. on Inform. Sci. and Syst. (CISS '06) (Princeton, NJ, 2006), pp. 857–863.

[4] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[5] S. Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[6] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru, "Secure network coding for wireless mesh networks: Threats, challenges, and directions, vol. 32, no. 2, pp. 121–125, Nov. 2009.

[7] Sudheer kumar and Shruthi Reddy, "Mixed signal based transmission in mixed layers for high throughput wireless network,"*Elixir online journal"vol-3*, pp. 7382–7385, Mar. 2012.

[8] A. Fiat, "Batch RSA," Crypto'89, pp.175-185, 1989, See also Journal of Cryptology, 10(2):75-88, 1997.

[9] R. Johnson, D. Molnar, D. Song, D. Wagner, Homomorphic signature schemes, Proceedings of RSA, Cryptographer's Track. LNCS 2271 (2002).

Books:

[10] T. S. Rappaport, presented at the Wireless Communications Principles and Practice 2nd edition.

Sudheer Kumar Battula

Received the Bachelor's degree from Aurora's Scientific and Technological Institute affiliated to JNTU Hyderabad University in 2009. I'm currently pursuing my Masters from the *Anurag* Group of Institutions affiliated to JNTU Hyderabad University in Computer Science & Engineering department.

P. Anjaiah

Received the Bachelor's degree from Aurora's engineering college bhongir, affiliated to JNTU Hyderabad University in 2004. Received M.Tech degree from SIT, jnt university,. in 2006. Currently working as a Asst. Professor in *Anurag* group of institutions affiliated to JNTU in C.S.E.