IJCTA, 10(02), 2017, pp. 41-43
© International Science Press

Authenticated Communication With Artificial Noise And Channel Coding using Quantization

Blessy Jenila.R* and Velmurugan.S*

Abstract : Authenticated communication refers to the communication among the valid end users.This can be done using Message Authentication code(MAC).Message authentication codes helps in the verification of message transmission among the authenticated users which leads to the strong privacy measurements. Message authentication codes is generated when the transmitter sends an message.MAC is the combination of message and the shared key which is known only to the transmitter and the receiver.At the receiver end the MAC is computed and compared with the relevant transmitted MAC.If the MAC at the transmitted and received end are same then it is said to be identical and the received message is equal to the message which is transmitted by the legal user.For the purpose of authentication two independent methods are proposed such as Information-theoretic authentication codes and Complexity-theoretic authentication codes.In this paper a new approach called Artificial-noise-Aided MACs(ANA-MACs) is proposed for ensuring both computational and theoretic securities.The use of Artificial noise in ANA-MACs makes it tough for the opponent to derive the key.Channel coding approach is enabled for the ease of key recovery problem.The quantization method helps to transmit the messages in packets above the physical layer.

Keywords : Physical layer, Artificial noise, Message Authentication codes, channel coding, Quantization.

1. INTRODUCTION

Information security is the most sensitive issue in message transmission .It is necessary to confirm that the received message truly comes from the desired transmitter .This leads to the high privacy concern and also saves the integrity of the transmitted message .Message authentication codes are used to confirm that the message comes from the legal user and ensures the integrity of the message.During message transmission the Message authentication code is generated and is known only to both the transmitter and the receiver.Authenticity can be achived using this shared key among the transmitter and the receiver.The artificial-noise-aided method proposed in the system enables to induce the artificial noise into the message which makes the opponent to derive the shared key.The message along with the noise and shared key can be transferred packets above the physical layer using quantization methodology. The key recovery problem in spoofing attacks of message authentication codes are more familiar in message transmission above physical layer.This problem can be eradicated using channel coding approach.

2. SYSTEM ANALYSIS

In the current situation ,authentication of transmitter and the receiver at the physical layer can be done using prior coordination or secret sharing.This kind of authentication authenticates the sender if the receiver can successfully decode the transmission.In physical layer authentication the messages along with MAC are transmitted over the physical layer.In the transmission of messages above the physical layer ,the possibility of theoretic security is very low due to the presence of channel noise and the security is

* Department Of Computer Science and Engineering Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai-62. *blessy.jenila@gmail.com, velmurugan@veltechmultitech.org*

based on the physical layer.The Artificial noise aided message authentication codes are encapsulated with messages and transmitted in packets above the physical layer using quantization.The linearity of codes helps in the reduction of complexity in message transmission.The hash functions are practically avoided due to their non linearity for the construction of message authentication codes.

3. PROPOSED SCHEME

The Confidentiality and Integrity of the message transmitted among the authenticated users are ensured using the message authentication codes.This paper proposes a new message authentication codes known Artificially noise aided message authentication codes(ANA-MACs).This proposed ANA-MACs are both computationally and theoretically secure.In ANA-MACs the artificial noise are interfered with the message authentication codes and transmitted.The transmission is done using quantization technique where the MAC along with noise are transmitted as packets above the physical layer.The proposed scheme is similar to the physical layer authentication scheme where the noise are added by the channel and hence cannot be controlled.The ANA-MACs overcomes this issue by introducing predefined amount of noise to the system and thus enhances the safe transmission of messages among authenticated users.

A. Artificial-Noise-Aided Mac

The Artificial noise aided message authentication codes are the proposed technique in which the noise are added artificially to the messages along with the shared key.Thus the message to be transmitted includes the valid message,shared key and the artificially induced noise.The normal encryption method enables the ease of key recovery if the opponent has the unlimited power of computation .This method will lead to the difficulty in key recovery attack .If suppose any opponent tries to recover the key by high computational power it leads to failure due to added artificial noise.Only the noise could be recovered and not the actal message.The main advantage of this method is the noise added could be controlled according to the message to be transmitted.

B. Channel Coding

The channel coding is the technique used to confirm the accuracy of the message transmitted. The integrity of message is ensured if and only if the transmitted message is of minimal or no errors.The standard authentication tags can be generated using channel coding and can be used for the ensembles of codes during message transmission.In channel coding technique the shared key is considered as an input and the message is used to specify a code from the entire collection of codes.

C. Quantization

The transmission of messages above the physical in the form of packets are more effective and can be done using quantization.Quantization is the process which maps the large set of input values to a smaller set and thus facilitates the packet transmission.The proposed system is similar to the traditional system where the message authentication codes are encapsulated in packets and transmitted above the physical layer.However the physical layer authentication schemes makes the prposed system to differ from the traditional message authentication codes.Quantzation has been very effective in the three performance metrics such as completeness error,false acceptance probability and the conditional equivocation about the key.

4. MODEL EVALUATION

The message along with the shared key is aided with artificial noise and are transmitted among the authenticated users.

The authenticated receiver could receive the message.If the intruder tries to access the message only the noise could be accessed and not the actual message. This in turn leads to the access of fake messages by the unauthorized users.Quantization helps in the transmission of messages in packets.The channel coding technology enables the key recovery in case of any fault in message transmissions.

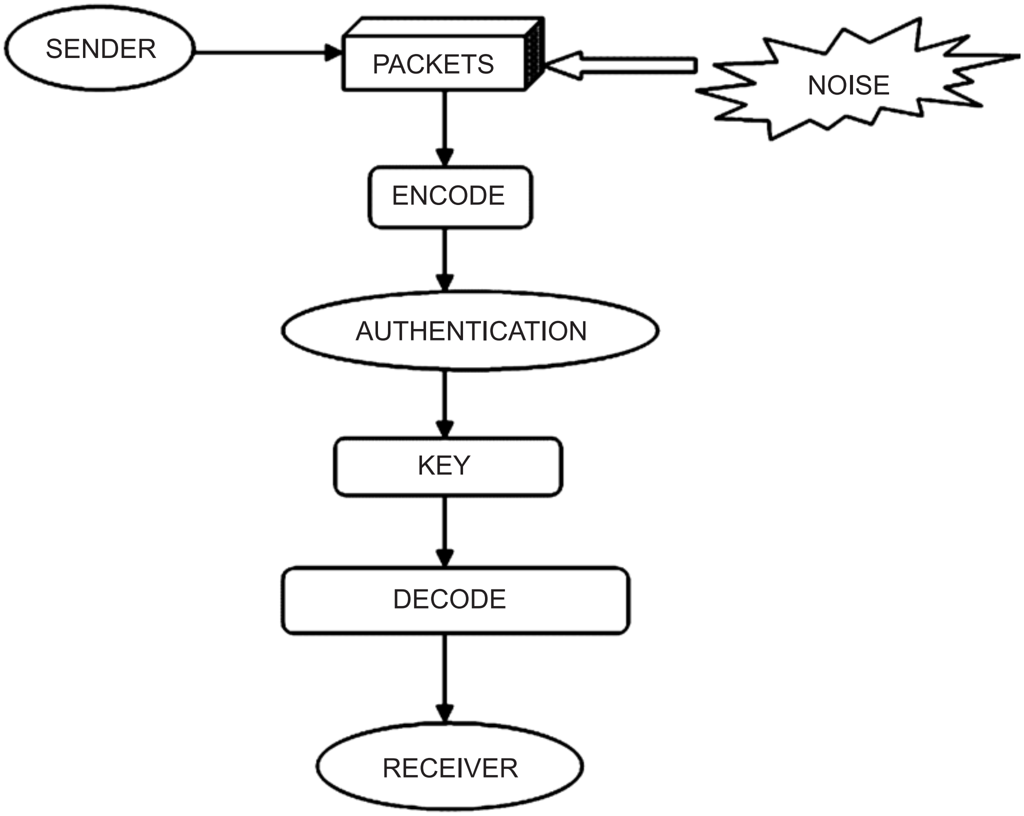

Figure 1: System Architecture

5. CONCLUSION

The authenticated message transmission with artificial noise enables the confidentiality and integrity of the transmitted message.It overcomes the traditional method with channel coding technique above the physical layer.Even if the intruder has unlimited power of computation ,the opponent could not recover the messages which increases the secured message transmission.

6. REFERENCES

1. R.F.Graveman and K.E.Fu,”Approximate message authentication codes”,in proc 3rd Annu Fedlab Symp.Adv. Telecommun./Inf.Distrib.,vol.1.Feb 1999,pp 1-5.
2. U.M.Maurer,”Authentication theory and hypothesis testing”,IEEE Trans.Inf.Theory,vol.46,no.4,pp 1350-1356,Jul 2000.
3. L.Xiao,L.J.Greenstein,N.B Mandayam and W.Trappe,”Using the physical layer for wireless authentication variant channels”IEEE Trans,Wireless Commun.,vol.7,no.7,pp.2571-2579,jul.2008.
4. M.Demirbas and Y.Song,”An RSSI-based schema for Sybil attack detection in wireless sensor networks using signal prints”,in proc International Workshop on Advanced Experimental activity,pp.564-570,june 2006.
5. D.Faria and D.Cheriton,”Detecting identity-based attacks in wireless networks using signal print “,in proc.ACM Workshop on wireless security,pp 43-52,Los angels,California,Sept.2006.
6. A.E Hero,”Secure space-time communication”,IEEE Transactions on Information theory,pp.3235-3249,December 2003.
7. L.Xiao,L.Greenstein,N.Mandayam and W.Trappe, Fingerprint in the ether:Using the physical layer for wireless authentication”,in proc IEEE International Conference on communications,Glasgow,Scotland,June 2007.
8. P.A.Bello,”Characterization of randomly time-variant linearchannels”,IEEE Trans commun syst,vol CS-11,pp.360-393,Dec1963.
9. W.C Jakes Jr.,Microwave mobile communications,Piscataway,NJ Prentice Hall,1996.
10. T.S.Rappaport,Wireless communications-principles and practice Englewood cliffs, NJ Prentice Hall,1996.