ANA-MAC and Quantization Method of Authenticated Communication

Blessy Jenila R, Bharathi S

Abstract*: Communication among valid end users is said to be auntheticated communication.Message authentication code enables this communication in well secured manner.The transmitted messages are verified by the message authentication codes,which inturn enhances the strong privacy measurements.The combination of message and the secret code is said to be Messaage Authentication Code (MAC).The shared key is known only to the transmitter and the receiver.The MAC received at the receiver end is verified for its originality.If it is same then it is inferred to be a original message.In order to ensure the computational and theoretic approach of securities an approach called Artificial Noise Aided MAC(ANA-MAC) is prposed for ensuring the theoretic and computational securities in transmission of messages.The use of Artificial noise in ANA-MACs results in difficulty for the intruder to derive the key.For the ease of key recovery by the receiver channel coding approach is enabled.In order to transmit the messages over physical layer,the quantizatiojn method is enabled.

Index Terms*: Artificial noise, Channel coding,Message Authentication code, Quantization.

I. INTRODUCTION

The most sensitive issue in message transmission is the Information security.Confirmation of message transmission from the appropriate sende is most important to preserve the aunthenticity.This leads to the high privacy and also saves the integrity of transmitted message.MAC is used to confirm that the message is transmitted from the legal users and thus ensures the integrity of message.The generated MAC during transmission is known only to the transmitter and the receiver.The ANA-MAC in the system enables to induce the artificial noise into the message which makes the intruder difficulty to derive the shared key.ANA-MAC can be encapsulated and transmitted in packets above the physical layer.A slight change in messages may result in rapid change for authentication tags.Since the messages are transmitted in packets by the method of quantization it enhances the completeness of transmitted message.The Channel coding approach enables the key recovery during attack in transmission.

II. SYSTEM ANALYSIS AND PROPOSED SCHEME:

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 receiver can successfully decode the transmission.During 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 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 MAC are used to ensure the confiedentiality and integrity of the message transmitted among the authenticated users.The ANA-MAC ensure the security of message transmission in both computational and theoretical measurements.The artificial noise are interfered with the message authentication codes and transmitted by using quantization technique.The transmission of messages using ANA-MAC overcomes the issue of message intrusion by inducing predefined amount of noise to the system and thus enhances the safe transmission of messages among authenticated users.

A. Artificial noise aided MAC

The transmission of messages using added artificial noise enables the high secrecy of message transmission.The message to be transmitted comprises of the valid message,shared key and the manually included noise.This method of added noise will lead to the difficulty in key recovery attack.The main advantage of this method is the transmitter could add noise as much as possible which leads to the failure in recovery of actual message by the intruder.

B. Channel coding

The integrity of message is ensured only if the transmitted message is of no errors,which can be done by using channel coding approach.The standard authentication tags can be generated using channel coding and can be used for ensembles of codes during message transmission.In this method 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

Quantization method enables the transmission of message in the form of packets above the physical layer.This method maps the large set of input values to a smaller set and thus facilitates the packet transmission.Quantization method is effective in three performance metrices such as completeness error,false acceptance probability and the conditional equivocation about the key.

Revised Manuscript Received on June 05, 2019

Blessy Jenila R, Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India.

Bharathi S, Department of Computer Science and Engineering, Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India.

III. ANA-MAC SYSTEM ARCHITECTURE

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. The message to be send are transmitted through packets along with the artificially aided noise. It is then encoded and transmitted using the key. With the use of shared secret key the messages are decoded and by the authenticated receiver. The opponent could retrieve only the noise and not the actual message. This leads to the fake message access by the unauthorized access.

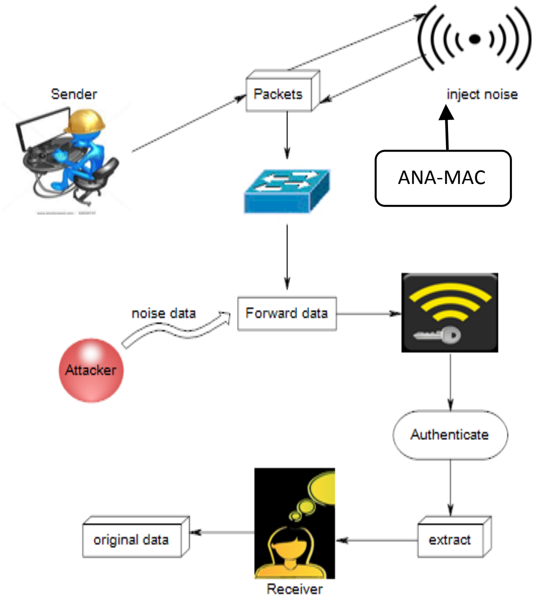

Fig . ANA-MAC system architecture

IV. ALGORITHM

A. Verification Algorithm

In considering the algorithm just developed the general case, i.e. there are numbers in the file, is checked first. After opening the file the current reading point is set at the first number. On entering the loop statement the current number is read and the reading point in the file is advanced to the next item. Ultimately the end-of-file marker will be the next item to be read and the condition `not at end of file' becomes false and exit is made from the loop. Hence all the numbers in the file are read but nothing more Hence as both these quantities start of at zero and the body of the loop is executed for each number in turn the accumulated total and number count must be correct, hence the average must be correct.

B. ANA-MAC Algorithm

The ANA-MAC algorithm provides an enhanced security by adding a artificial noise added to the original piece of information i.e,the quantity of noise added is same as that of the information to be transmitted.The noise added includes some special characters and hence it makes the opponent difficult to retrieve the original data.The artificial noise is interfered with clean data and then quantization is used to facilitate the packet transmission.The Artificial noise aided message is thus with a probabilistic algorithm to produce the information with noise and the original message to be transmitted.

C. Routing Algorithm

The decision of message forwarding in Routing protocol is mainly based on the goodness of the encountered node regarding the destination, and the number of message copy tokens. If the message tokens greater than 1, weighted copy rule is applied, the forwarding rule is applied otherwise.

V. MODULES DESCSRIPTION

A. Network creation

The use of artificial noise in ANA-MAC makes it difficult for an opponent to derive the key.With the use of quantization,ANA-MAC can be encapsulated and transmitted in packets aove the physical layer,just like the traditional MAC which is in sharp contrast to existing physical layer authentication schemes.It should be pointed out that the proposed ANA-MAC are also different with the binary approximate messsage authentication codes and the noise tolerent message authentication codes.Both AMAC and NT-MAC are designed to tolerate some channel errors during the transmission of messages.

B. Communication link

The opponent should do the best to generate a clear authentication tag , instead of a noise-corrupted version , given that has been observed for a spoofing attack of order. Indeed, if an illegal tag is generated by the opponent, the introduction of artificial noise may slightly increase the false acceptance probability. However, this increase is often minor as the false acceptance probability should be less than a small target value.one should carefully balance the three performance metrics, namely, the successful authentication probability, the false acceptance probability and the security against spoofing attacks

C. Scheduling

The sphere-packing bound of Shannon provides a lower bound on the decoding error probability of block codes transmitted over the BI-AWGN channel. With a coding approach for MACs, the best possible recovery of key for a potential eavesdropper to attack ANA MACs is to use an ML decoder, with which, the decoding probability can be lower bounded with the Shannon’s sphere-packing bound.

D. Services and extraction

To facilitate packet transmission, quantization should be introduced for ANA-MACs. As the previous analysis assumes no quantization, it is essential to consider the effect of quantization on the three performance metrics, namely, the completeness error, the false acceptance probability, and the conditional equivocation about the key.

VI. PERFORMANCE AND EVALUATION:

A. Performance

Performance describes how the performance is increased while transmitting packets between two ends.If an intruder attacks a port ,the port number is changed for improved security.Improving this kind of security by changing port there is a success full transmission of packages.Port attack may lead to delay.After that time delay is gradually increased it enables the intruder to attack easily.Hence by changing the port the attack gets reduced and thus improves the packet transmission.

B. Comparison

The comparison is all about the packet delivery ratio of existing system and the proposed system.Due to port attack there is a decrease in packet delivery ratio in the existing system.In proposed system the attacked port could be changed and updated.This reduces the delay in packet delivery and hence improves the packet delivery ratio.

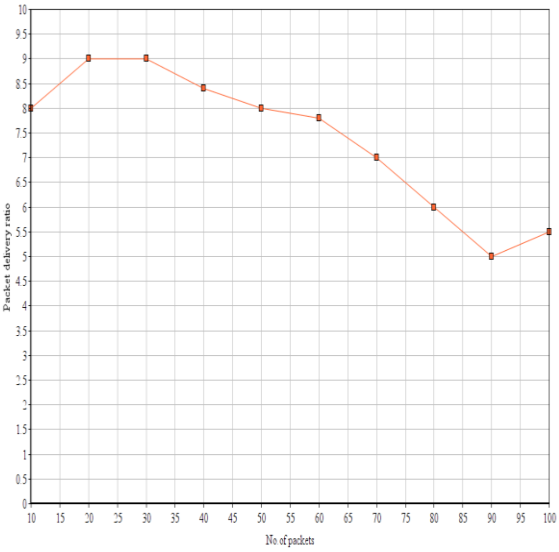

Fig : Packet Delivery ratio of Existing system

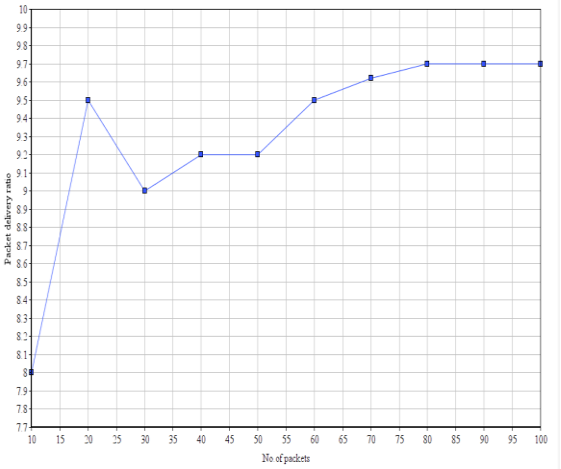

Fig : Packet Delivery ratio of Proposed system

VII. 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. The use of artificial noise in ANA-MACs makes it difficult for an opponent to derive the key. With the use of quantization, ANA-MACs can be encapsulated and transmitted in packets above the physical layer, just like the traditional MACs, which is in sharp contrast to existing physical layer authentication scheme AMACs and NT-MACs are computationally secure,while ANA-MAC may ensure some degree of information theoretic security.In future theoretical methods can be applied in order to prevent the attacks in port.Alternate techniques should be adopted in order to improve the performance ratio and to enhance the security in message transmission.

REFERENCES

1. Bello.P.A,“Characterization of randomly time-variant linear channels”, IEEE Trans commun syst,vol CS-11,pp.360-393,Dec1963.
2. Demirbas.M and Song.S, “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.
3. Faria.D and Cheriton.D, “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.
4. Graveman.R.F and Fu.K.E, “Approximate message authentication codes”, in proc 3rd Annu Fedlab Symp.Adv.Telecommun./Inf.Distrib.,vol.1.Feb 1999,pp 1-5.
5. Hero.A.E, “Secure space-time communication”, IEEE Transactions on Information theory,pp.3235-3249,December 2003.
6. Jakes.W.C Jr., “Microwave mobile communications”, Piscataway , NJ Prentice Hall,1996.
7. Maurer.U.M, “Authentication theory and hypothesis testing”, IEEE trans. Inf. Theory vol.46,no.4,pp1350-1356,Jul 2000.
8. Rappaport.T.S, “Wireless communications-principles and practice Englewood cliffs”, NJ Prentice Hall,1996.
9. Xiao.L,Greenstein.L,Mandayam.N and Trappe.W, “Fingerprint in the ether:Using the physical layer for wireless authentication” ,in proc IEEE International Conference on communications,Glasgow,Scotland,June 2007.
10. Xiao.L,Greenstein.L.J, Mandayam.N.B and Trappe.W, “Using the physical layer for wireless authentication variant channels” IEEE Trans, Wireless Commun.,vol.7,no.7,pp.2571-2579,jul.2008.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication