International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Wireless Communication Security Through Symbol Obfuscation in Physical Layer

S.Niranjani[1], R.Nirmalan[2]

[1] *PG Scholar,Department of CSE,Sri Vidya College of Engineering and Technology,Virudhunagar,TN,India*
[2] *Assistant professor,Department of CSE,Sri Vidya College of Engineering and Technology,Virudhunagar,TN,India*

Abstract - ***Secure communication is a critical and challenging issue in wireless networks. To achieve the information theoretic secrecy the leading approach is artificial noisy symbol. The basic idea in this paper is enhancing the security in wireless communication. Multiple Inter-symbol Obfuscation(MIO) method will be deployed in the physical layer. MIO is a method for transferring the data and it provides security in wireless network. The possibility of symbol obfuscation is to eliminate the eavesdropper participation and the fake packet injection. The original data symbols are obfuscated by using set of symbol keys. The information theoretic secrecy will be achieved and the other hand an eavesdropper cannot able to decrypt the original data symbols. The legitimate receiver can easily check the original data symbols and reject the fake packet injection during the data transmission.***

Keywords: *Wireless communication security, Physical layer, Multiple inter-symbol obfuscation, Information theoretic secrecy.*

1. INTRODUCTION

Wireless communication is an extending portion in communication technology. It is a method for transferring information between multiple systems. Wireless connectivity between computers, phones and security systems will be processed by the use of internet. Wireless sensor have a vast use in commercial application such as monitoring of fire hazard, carbon dioxide movement, military application such as identification and tracking of enemy targets, counter terrorism. The critical challenge of wireless communication is the privacy protection and authentication by using public-key and private-key cryptograpy. In addition, wireless mediums are vulnerable due to vicious message injecting and eavesdropping. Most security schemes have been implemented in the upper layer. In this wireless communication unauthorized receiver can easily access the transmitted data. Recent analysis shown that physical layer security become a crucial part in wireless communication.

Physical layer security analysis falls in three areas such as channel coding approaches, signal design approaches, artificial noise approaches for secure communication. This work examines a security technique like MIO in physical layer. The wireless medium will be secured by transmitting an artificial noisy symbols. It expose that the proposed technique enhances the security rather than other security methods which will implemented in the upper layer of communication network.

In MIO scheme the two attackers are passive eavesdropping attack and fake packet injection attack. In this the original data symbols are obfuscated by using set of artificial noisy symbol(symbol keys). MIO does not need to trust any third party to set up the symbol keys. In this mechanism appropriate transmitter can randomly encrypt the original data symbols without any apprise to the appropriate receiver. The receiver has to utilize the key checking process to discover the symbol key's position. MIO can allow the appropriate receiver to decrypt the encrypted symbol. Multiple inter-symbol obfuscation provide information-theoretic secrecy and fake packet injection attack. In MIO method the two attackers are passive eavesdropping attack and fake packet injection attack.

Multiple Inter-symbol Obfuscation includes two stages such as MIO encryption and MIO decryption. MIO encryption adding artificial noisy symbol key into original data symbols. MIO decryption offsetting the artificial symbol key in the encrypted data symbol to obtain the original data. The corrupted packets will be drop by using Cyclic Redundancy Check(CRC). If the data packets are received correctly in the receiver side then the acknowledgement will send back to the transmitter otherwise the receiver drop the corrupted packets by using CRC and waits for packet retransmission.

2. LITERATURE SURVEY

In 2012 Mohammad Iftekhar Husain et. al explained that the constellation diversity of wireless networks exploits by using physical layer security. They introduces CD-PHY technique that will be based on constellation diversity which is not depend on channel characteristics. They specified custom bit sequence to constellation symbol mapping for the legitimate transmitter and receiver to secure the physical layer communication. This symbol mapping act as a secret key for secure communication. They describes that CD-PHY provide security much stronger than modulation types. They exposed that in the presence of CD-PHY the eavesdropper have low probability to decode the original signal[1]. In 2005 Tongtong Li et.al analysed the physical layer security weakness of the IS-95 CDMA airlink interface. They proposed secure scrambling to improve the physical layer built-in security of CDMA system based on Advanced Encryption Standard (AES). Data Encryption Standard(DES) will be used as a criterion to assess the security of the proposed secure scrambling. The described that information privacy and system performance can be improved that the training sequence and message sequence can be scrambled separately with two independent scrambling sequences[2].

In 2011 Shyamnath Gollakota et.al explained the physical layer approach to achieve the secret key that is fast and independent of channel variations. Channel-independent PHY technique will be introduced and namely Ijam that assure that an eavesdropper cannot able to demodulate a wireless signal. They explained Ijam as the sender repeats its transmission, the receiver jams the original transmission sample or the corresponding sample in repetition[3]. In 2009 Xiangyun Zhou et.al considered the problem of communication security in wireless fading channel in the existence of non-colluding eavesdropper channel. An analytical closed-form lower bound for secrecy capacity will be obtained and that will used as the objective function to upgrade transmit power allocation between the artificial noise and the information signal. They found channel realization based adaptive power allocation that provides insignificant capacity improvement. They investigated the optimal transmit power allocation between information bearing signal and the artificial noise by using closed-form capacity expression as objective function[4].

In 2012 Arsenia Chorti et.al explored the resilence of multi-user network to active and passive eavesdropping. They inspected the scenario of passive eavesdropping without availability of the side information. They investigated the active eavesdropping which we formulate as a one-shot two player zero-sum game. They explained about the average Secrecy Capacity(SC) in two method that is (i)without side information and (ii)with side information. They systematically evaluated the effect of an active eavesdropper by using game theoretic tools[5]. In 2007 Ruoheng Liu et.al considered the issue of secure coding design for type II wiretap channel. They focused on secure coding scheme for a type II wiretap channel in this the main channel is noiseless and the eavesdropper channel is Binary-Input Symmetric-Output Memoryless(BISOM) channel. A secure error-correcting code will be proposed in terms of nested code structure. They derived the corresponding achievable rate-equivocation pair based on threshold behaviour of good code sequence. They derived a perfect secrecy rate by extending a secure coding to a type II wiretap channel[6].

In 2000 Bijan G. Mobasseri proposed to use the constellation shape for robust signature that will be used to the digital modulation recognition. The transmitted information will be represented by the geometry of the constellation. Fuzzy c-means clustering is demonstrated to robust recovery of the unknown constellation. Bayesian inference will be performed by the reconstructed constellation that is modelled by a discrete multiple-valued non homogeneous spatial random field. The received signal constellation is a multidimensional, multiclass random process[7]. In 2006 Desmond S. Lun et.al presented a specific coding scheme and specific distributed flow optimization techniques that they form a basis of protocol. They suggested practicable distributed method that will perform in practical situation to implement coding. Five different approaches like End–to-End retransmission, End-to-End coding, Link-by-Link retransmission, Path coding, Full coding will be considered by them. They provided a distributed approach to solve the problem of establishing efficient unicast connection[8].

In 2008 Dong Nguyen et.al considered network coding applications to enhance the bandwidth efficiency of reliable broadcast in wireless network. Various retransmission broadcast scheme are explained with and without network coding. Memoryless Receiver broadcast scheme without network coding and Time-Based Retransmission broadcast scheme with network coding will be described by them. Network coding will be employed to exchange the information in wireless network. For the information exchange between two wireless nodes they used XOR operation. Different lost packet from different receiver are combined to recover the lost packets in one transmission by a multiple receiver[9]. In 2008 Matthieu Bloch et.al considered the transmission of confidential data over wireless channel. To achieve communication rates they introduced optimal Low-Density Parity-Check(LDPC) Codes. They developed secure communication protocol to ensure wireless information-theoretic secrecy which used four steps: common randomness vs opportunistic transmission,

message reconciliation, common key generation, message protection with secret keys. The key agreement protocol will be illustrated and also presented a reconciliation procedure based on multilevel coding and LDPC codes. The secret key agreement protocol will be extended to allow for imperfect channel state information. Wireless system setup will be considered when a legitimate wants to send messages to other user. The impact of fading on secure communication will be considered by two metrics such as average secrecy capacity and probability of outage of secrecy capacity[10].

In 2011 Frederique oggier et.al described about MIMO wiretap channel. Based on a generalization of the wire-tap channel to MIMO broadcast wire-tap channel the problem of computing the perfect secrecy capacity will be considered. When the legitimate transmitter and receiver can communicate at positive rates the perfect secrecy will be achieved. The secrecy capacity of the multiple antenna wire-tap channel will be computed. A proof technique for the converse will be provided in order to secrecy capacity computation[11]. In 2002 Srikrishna Bhashyam et.al derived the maximum-likelihood channel estimate for long-code CDMA systems and used an iterative algorithm to reduce computational complexity in each symbol duration. They described the ML channel estimation technique that provides an estimate of the effective channel impulse response. For multiuser channel estimation they applied gradient-based adaptation technique by using exact gradient. Two iterative algorithm will be explained to approximate the ML solution like simple gradient descent algorithm and steepest descent algorithm[12].

3. CONCLUSION

In this paper we considered the solution for secure wireless communication in data transmission. We can achieve this secrecy by implementing Inter-symbol obfuscation scheme in physical layer. We considered that artificial noisy symbol will be employed in the original data symbol. The dynamic symbol key updating will be considered for the symbol obfuscation to prevent information from passive eavesdropping and malicious message injection.

REFERENCES

[1] M. I. Husain, S. Mahant, and R. Sridhar, "CD-PHY: Physical layer security in wireless networks through constellation diversity", in *Proc IEEE MILCOM*, Oct./Nov. 2012, pp. 1–9.

[2] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems", in *Proc. IEEE MILCOM*, Oct. 2005, pp. 956–962.

[3] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent", in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1125–1133.

[4] Xiangyun Zhou, Matthew R. McKay, "Physical Layer Security with Artificial Noise Secrecy Capacity and Optimal Power Allocation", in proc. *IEEE ICSPCS*, Sep.2009, pp. 1 – 5

[5] Arsenia Chorti, Samir M. Perlaza, Zhu Han, H. Vincent Poor, "Physical Layer Security in Wireless Networks with Passive and Active Eavesdroppers", in *proc. IEEE GLOCOM,* Dec*. 2012,* pp. 4868 – 4873

[6] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevi´c, "Secure nested codes for type II wiretap channels", in *Proc. IEEE Inf. Theory Workshop*, Sep. 2007, pp. 337–342.

[7] B. G. Mobasseri, "Digital modulation classification using constellation shape", *Signal Process.*, vol. 80, no. 2, pp. 251–277, Feb. 2000.

[8] Desmond S. Lun , Muriel M´edard & Ralf Koetter, "Network Coding for Efficient Wireless Unicast", in *proc.* Feb 2006, pp. 74-77.

[9] Dong Nguyen,Thinh Nguyen, Bella Bose, "Wireless Broadcasting Using Network Coding", in proc. IEEE TVT, June 2008, pp. 914 – 925.

[10] Matthieu Bloch, João Barros, Miguel R. D. Rodrigues, Steven W. McLaughlin, "Wireless Information-Theoretic Security", in proc. IEEE TIT, June 2008,pp. 2515 – 2534

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel", *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972,Aug. 2011.

[12] S. Bhashyam and B. Aazhang, "Multiuser channel estimation an tracking for long-code CDMA systems", *IEEE Trans. Commun.*, vol. 50,no. 7, pp. 1081–1090, Jul. 2002.