BER-BASED PHYSICAL LAYER SECURITY BY COMBINING STRONG CONVERSE AND ERROR AMPLIFICATION

[1]Dharani M, [2]Dhivya Anoo S, [3]Khaviya G S, [4]Dr. D. Surendran

[1,2,3,4] Department of Computer Science and Engineering,

Sri Krishna College of Engineering and Technology

[4]surendran@skcet.ac.in

Abstract

The BER based physical layer security is used for the systems which use TDMA based MAC protocol with dynamically allocated Time slots. In contrast with CCC (Common Control Channel) based MAC protocols, TSAMAC (Time Slot Allocation MAC) protocol is based on the TDMA mechanism, without using any CCC for control information exchange. The channels are divided into time slots and users send their control or data packets over their designated slot. TSAMAC is improve the throughput of the communication channel for the unlicensed user. This method will facilitate to decide and allocate free channel to secondary user without interfering with primary user. The protocol ensures that no slot is left vacant. This guarantees full use of the available spectrum. The protocol includes the provision for Quality of Service, where real-time and safety critical data is transmitted with highest priority and least delay.

I.INTRODUCTION

Security during the data transmission in the physical layer usually done with the block error probability where in the transmission rate should always be greater than the channel capacity. This is because we statically fix the transmission rate without using protocols dynamically. Fixing the transmission rate statically will make it easy to trace the data sent during transmission and as a result security will not be ensured accurately. Thus the concept of using timeslot allocation protocols and allocating the transmission rate dynamically depending upon the size of the text using Bit Error Rate.

For secure communication in the sense of high BER, the information- theoretic strong converse is combined with cryptographic error amplification achieved by the substitution permutation networks based on the confusion and diffusion. For the discrete memory less channels (DMCs), an analytical framework is provided showing the tradeoffs among the finite block length, the maximum/minimum possible transmission rates, and the BER requirements for the legitimate receiver and the eavesdropper.

In addition, the security gap is analytically studied for the Gaussian channels and the concept is extended to other DMCs including the binary symmetric channels and binary erasure channels.

The channels are divided into time slots and users send their control or data packets over their designated slot. TSAMAC is improve the throughput of the communication channel for the unlicensed user. This method will facilitate to decide and allocate free channel to secondary user without interfering with primary user. The protocol ensures that no slot is left vacant. This guarantees full use of the available spectrum. The protocol includes the provision for Quality of Service, where real-time and safety critical data is transmitted with highest priority and least delay.

SECURITY is a critical issue in communications, which has been traditionally

addressed at a higher layer by cryptography. As a fundamentally different approach, the physical layer security, particularly information theoretic security, has received a lot of attention. Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connect and transfer information.

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. Due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore, the network topology changes from time to time.In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing.

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols – the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols. However, there is not a complete routing protocol that can secure the operation of an entire network in every situation. Typically, a "secure" protocol is only good at protecting the network against one specific type of attacks.

Many researches have been done to evaluate the performance of secure routing protocols in comparison with normal routing protocols. One of the objectives of this research is to examine the additional cost of adding a security feature into non-secure routing protocols in various scenarios. The additional cost includes delay in packet transmission, the low rate of data packets over the total packets sent, etc.

It is well known that the real-world network does not operate in an ideal working environment, meaning that there are always threats and malicious actions affecting the performance of the network. Thus, studying the performance of secure routing protocols in malicious environments is needed in order to effectively evaluate the performance of those routing protocols.

II.BIT ERROR RATE

The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unit less performance measure, often expressed as a percentage.

As an example, assume this transmitted bit sequence:

0 1 1 0 0 0 1 0 1 1

and the following received bit sequence:

0 0 1 0 1 0 1 0 0 1,

The number of bit errors (the underlined bits) is, in this case, 3. The BER is 3 incorrect bits divided by 10 transferred bits, resulting in a BER of 0.3 or 30%.

III.ANALYSIS OF BER

The BER may be evaluated using stochastic (Monte carlo) computer simulations. If a simple transmission channel model and data source model is assumed, the BER may also be calculated analytically. An example of such a data source model is the Bernoulli source.

Examples of simple channel models used in information theory are:

- Binary symmetric channel (used in analysis of decoding error probability in case of non-bursty bit errors on the transmission channel)
- Additive white guassian noise (AWGN) channel without fading.

A worst-case scenario is a completely random channel, where noise totally dominates over the useful signal. This results in a transmission BER of 50% (provided that a Bernoulli binary data source and a binary symmetrical channel are assumed, see below).

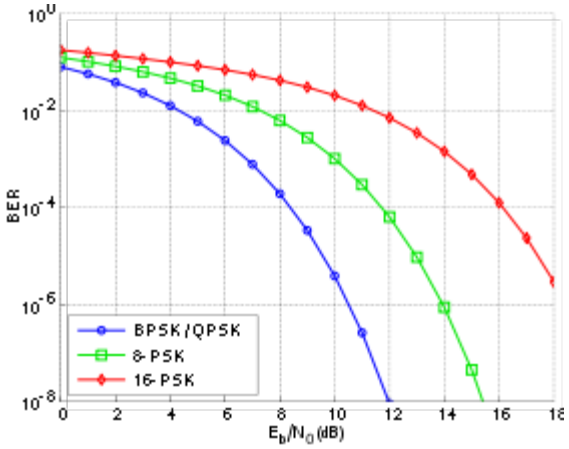

Fig 1. Bit-error rate curves for BPSK, QPSK 8-PSK and 16-PSK, AWGN channel.

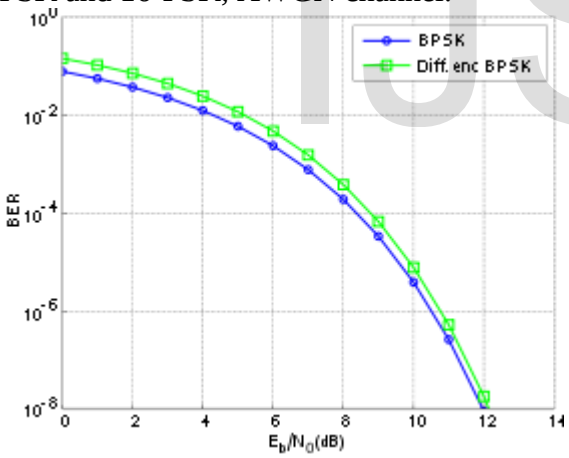

Fig 2. BER comparison between BPSK and differentially encoded BPSK with gray-coding operating in white noise.

In a noisy channel, the BER is often expressed as a function of the normalized carrier-to-noise ratio measure denoted Fb/N0,0000 (energy per bit to noise power spectral density ratio), or Es/N0(energy per modulation symbol to noise spectral density).

People usually plot the BER curves to describe the performance of a digital communication system. In optical communication, BER(dB) vs. Received Power(dBm) is usually used; while in wireless communication, BER(dB) vs. SNR(dB) is used.

Measuring the bit error ratio helps people choose the appropriate forward error correction codes. Since most such codes correct only bit-flips, but not bit-insertions or bit-deletions, the Hamming distance metric is the appropriate way to measure the number of bit errors. Many FEC coders also continuously measure the current BER.

A more general way of measuring the number of bit errors is the Levenshtein distance. The Levenshtein distance measurement is more appropriate for measuring raw channel performance before frame synchronization, and when using error correction codes designed to correct bit-insertions and bit-deletions, such as Marker Codes and Watermark Codes.

IV. ROUTE DISCOVERY PHASE

The proposed TDMA based MAC protocol with dynamically allocated Time slots. In contrast with CCC based MAC protocols, TSAMAC (Time Slot Allocation MAC) protocol is based on the TDMA mechanism, without using any CCC for control information exchange. The channels are divided into time slots and CR users send their control or data packets over their designated slot. TSAMAC is improve the throughput of the communication channel for the unlicensed user. This method will facilitate to decide and allocate free channel to secondary user without interfering with primary user. The protocol ensures that no slot is left vacant. This guarantees full use of the available spectrum. The protocol includes the provision for Quality of Service, where real-time and safety critical data is transmitted with highest priority and least delay.

The hybrid carrier-sense multiple access (CSMA)/time-division multiple access (TDMA) medium access control (MAC) protocol

combines the strengths of CSMA and TDMA protocols. In this letter, we propose a dynamic queue-length-based time slot allocation scheme for the hybrid CSMA/TDMA MAC protocol to improve channel utilization considering the uncertainty in queue length information. Due to the lack of a dedicated control channel from a device to the coordinator, the queue length in a device can be reported to the coordinator only in an intermittent manner. To overcome this difficulty, the proposed scheme calculates the probability mass function (pmf) of the distribution of the queue length and allocates slots during the TDMA period based on this pmf. The simulation results show that the proposed slot allocation scheme outperforms the time slot allocation scheme which does not take into account the distribution of the queue length.

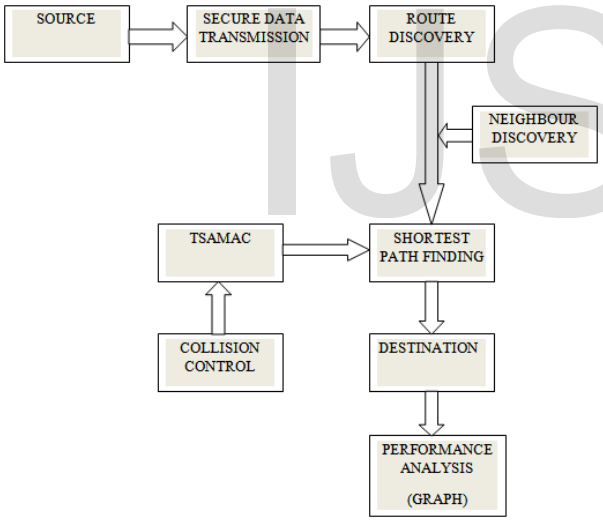

Fig 3. Block diagram of the proposed system

V. MANET NETWORK DEPLOYMENT

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

A MANET is an autonomous collection of mobileusers that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the nodes themselves must execute the topology and delivering messages, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETS is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETS need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETS.

VI. DATA COMMUNICATION

This Module is developed to MANET networks data communication and aggregation process. The radio and IEEE 802.11 MAC layer models were used. The network based data processing or most expensive and data communication level on their performance on the network. Multiple sources create and end sending packets. In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that have been altered due to noise, interference, distortion or bit synchronization errors. The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied

time interval. BER is a unit less performance measure, often expressed as a percentage.
The bit error probability is the expectation value of the bit error ratio. The bit error ratio can be considered as an approximate estimate of the bit error probability. This estimate is accurate for a long time interval and a high number of bit errors.

A MANET may include data pull, data push and peer-to-peer communication. No research has been done which includes all three forms of communication. However, data push and data pull have been addressed to varying degrees. Recent work in Mobile Ad-Hoc data communication is addressed. Their approach is the construction of a minimum-energy tree rooted at the broadcast source.

VII. TSAMAC

This module is developed to novel TDMA based MAC protocol with dynamically allocated Time slots. In contrast with CCC based MAC protocols, TSAMAC (Time Slot Allocation MAC) protocol is based on the TDMA mechanism, without using any CCC for control information exchange. The channels are divided into time slots and CR users send their control or data packets over their designated slot.

The proposed system uses TDMA based MAC protocol with dynamically allocated Time slots. In contrast with CCC (Common Control Channel) based MAC protocols, TSAMAC (Time Slot Allocation MAC) protocol is based on the TDMA mechanism, without using any CCC for control information exchange. The channels are divided into time slots and users send their control or data packets over their designated slot. TSAMAC is improve the throughput of the communication channel for the unlicensed user. This method will facilitate to decide and allocate free channel to secondary user without interfering with primary user. The protocol ensures that no slot is left vacant. This guarantees full use of the available spectrum. The protocol includes the provision for Quality of Service, where real-time and safety critical data is transmitted with highest priority and least delay.

VIII. PERFORMANCE ANALYSIS

This module is developed to improve Wireless network performance, Reduce Average end –to-end delay.

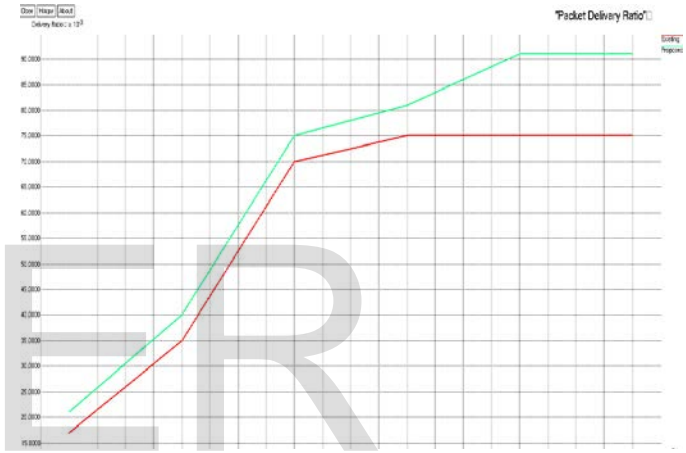

Fig 4. Packet delivery ratio

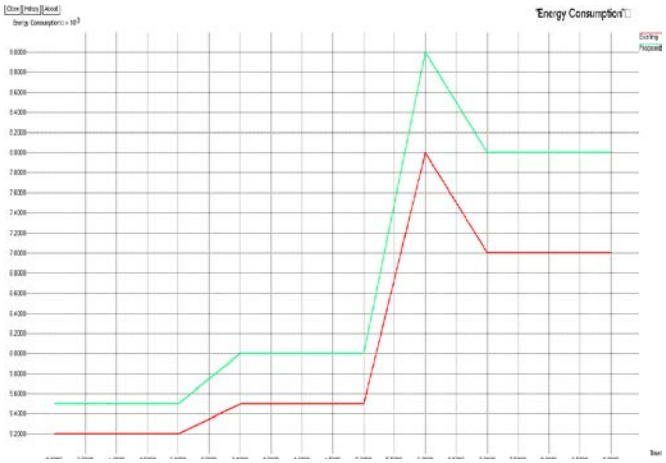

Fig 5. Energy consumption

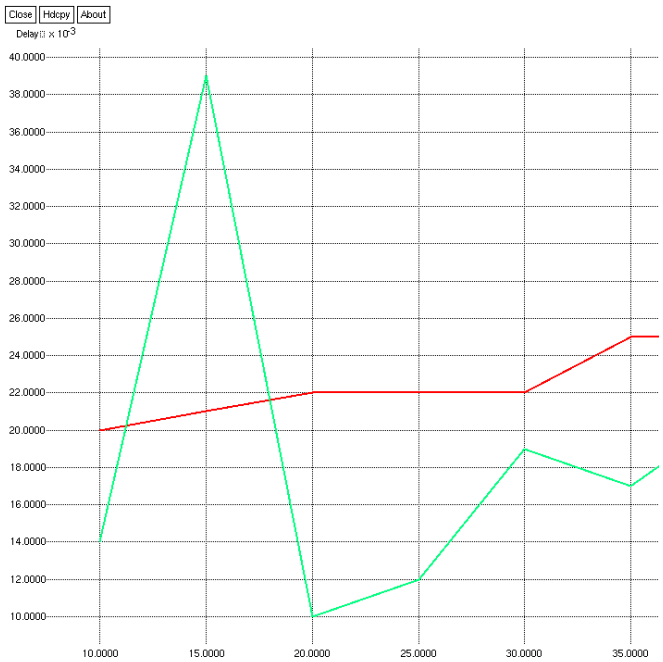

Fig 6. Average end to end delay

Fig 7. Throughput Ratio

IX. CONCLUSION

In this paper, a secure data transmission method has been studied, where the security measure was given in terms of the BER at the eavesdropper. To realize such secure communication, the information-theoretic strong converse and the cryptographic error amplification have been combined. For finite blocklengths, the maximum and minimum allowable transmission rates and the security gap have been analyzed for any block codes over the DMCs. It has been observed that increasing the blocklength is very effective to reduce the rate loss and the security gap. The most common security measure is the equivocation or equivocation rate. As a further work, therefore, it is an interesting issue to establish the relationship between the high BER criterion and the equivocation criterion. Once the relationship is established, the next interesting problem can be developing the secure communication mechanism jointly using the BER and equivocation criteria as for security.

In the, a secure data transmission method has been studied, where the security measure was given in terms of the BER at the eavesdropper. To realize such secure communication, the information-theoretic strong converse and the cryptographic error amplification have been combined. For finite block lengths, the maximum and minimum allowable transmission rates and the security gap have been analyzed for any block codes over the DMCs. It has been observed that increasing the block length is very effective to reduce the rate loss and the security gap. the most common security measure is the equivocation or equivocation rate. As a further work, therefore, it is an interesting issue to establish the relationship between the high BER criterion and the equivocation criterion. Once the relationship is established, the next interesting problem can be developing the secure communication mechanism jointly using the BER and equivocation criteria as for security.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, pp. 1355–1387, Oct. 1975.

[3] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[4] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[5] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[6] V. Rathi, M. Andersson, R. Thobaben, J. Kliewer, and M. Skoglund, "Performance analysis and design of two edge-type LDPC codes for the BEC wiretap channel," IEEE Trans. Inf. Theory, vol. 59, no. 2, pp. 1048–1064, Feb. 2013.

[7] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," IEEE Trans. Inf. Theory, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[8] A. Subramanian, A. Thangaraj, M. Bloch, and S. W. McLaughlin, "Strong secrecy on the binary erasure wiretap channel using largegirth LDPC codes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 585–594, Sep. 2011.

[9] M. Cheraghchi, F. Didier, and A. Shokrollahi, "Invertible extractors and wiretap protocols," IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 1254–1274, Feb. 2012.

[10] M. Bloch and J. Barros, Physical-Layer Security. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[11] U. M. Maurer, "The strong secret key rate of discrete random triples," in Communications and Cryptography—Two Sides One Tapestry, R. E. Blahut, D. J. Costello, Jr., U. Maurer, and T. Mittelholzer, Eds., Boston, MA, USA: Spiner-Verlag, 1994, pp. 271–285.

[12] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 1807. Berlin, Germany: Springer-Verlag, May 2000, pp. 351–368.

[13] C. W. Wong, T. F. Wong, and J. M. Shea, "LDPC code design for the BPSK-constrained Gaussian wiretap channel," in Proc. Globecomm, 2011, pp. 898–902.

[14] M. Baldi, F. Chiaraluce, N. Laurenti, S. Tomasin, and F. Renna, "Secrecy transmission on parallel channels: Theoretical limits and performance of practical codes," IEEE Trans. Inf. Forensics Security, vol. 9, no. 11, pp. 1765–1779, Nov. 2014.

[15] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in Proc. ICC, 2015, pp. 435–440.