Project	**IEEE 802.20 Working Group on Mobile Broadband Wireless Access** <http://grouper.ieee.org/groups/802/20/>
Title	**An Alternative Approach for Enhancing Security of WMANs using Physical Layer Encryption**
Date Submitted	**2003-09-05**
Source(s)	Arpan Pal Center of Excellence for Embedded Systems Tata Consultancy Services SDF Building, 3rd Floor Salt Lake Electronics Complex Kolkata – 700091 India Voice: +91-33-23339730 Fax: +91-33-23571074 Email: arpan_pal@tcscal.co.in
Re:	MBWA Call for Contributions
Abstract	Wireless Networks, and more specifically Wireless MANs are prone to security hazards. This paper proposes an alternate method of encryption at the physical layer, which can improve the security of Wireless MANs.
Purpose	Address security issues in a Wireless MAN
Notice	This document has been prepared to assist the IEEE 802.20 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.20.
Patent Policy	The contributor is familiar with IEEE patent policy, as outlined in Section 6.3 of the IEEE-SA Standards Board Operations Manual <http://standards.ieee.org/guides/opman/sect6.html#6.3> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/guide.html>.

Table of Contents

1 Introduction 3
2 Security Threats 3
3 Brief Description of the Scheme 3
4 Detailed Description 5
4.1 Existing Systems 5
4.2 Proposed System 6
4.2.1 Features 7
4.2.2 Example 7
4.2.3 Application to 802.20 8
5 Security Aspects mitigated by proposed scheme 8
5.1 Data Privacy 8
5.2 Data Forgery 8
5.3 Denial of Service 9
6 Summary 9

List of Figures

Figure 1 Existing Communication System Block Diagram 5
Figure 2 Proposed Communication System Block Diagram 6

References:

[1] Alan Chickinsky, “Wireless Security Threats”, IEEE C802.20-03/06, January 2003

[2] “Draft Supplement to Standards (for) Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Further Higher Data Rate Extension in the 2.4 GHz band”, IEEE P802.11g, D8.1, April 2003

1 Introduction

The existing security mechanism of WMANs is based on some sort of encryption with a keystream. Both transmitting and receiving parties know one part of the keystream called the secret key and it does not change frequently. Another part of the keystream is called Initial Vector (IV), which is changed every packet. But the IV is also sent in the open so that the receiving parties know which IV has been used.

This form of security is always prone to security attacks. There are suggested as possible ways of reducing security threat but obviously they are not foolproof.

The basic reason why this security attacks are easy to implement is the fact that anybody with a WMAN Network Interface Card (NIC) working in promiscuous mode attached to his laptop can snoop on the network and record data over a long time. Then by analyzing the data, the hacker can easily decrypt the actual data.

An alternate method of encryption is being that can enhance WMAN security.

2 Security Threats

The different ways the security of a WMAN can be compromised. They are outlined in detail in [1]. There can be following types of security events –

- Human Initiated Events
- Data Privacy
- Data Forgery
- Denial of Service
- Hardware Errors

Out of these, nothing can be done for security events that occur for human mistakes. Hardware errors occurring due to reception of wrong signals form a different class of problem, and hence can be handled in a different way. The proposed method tries to address security issues arising from the other three events, viz. Data Privacy, Data Forgery and Denial of Service.

3 Brief Description of the Scheme

The key to enhancing security lies in the prevention of recording the WMAN data by a hacker who is using standard WMAN NIC hardware. All WMAN Physical Layer protocols use different physical layer configurations like encoding rates and modulation schemes to achieve different data rates. The transmitter sends the information regarding which physical layer configuration is used to the receiver at the beginning of the packet. This information is sent using a pre-determined physical layer configuration so that the

receiver can understand this information. All the subsequent packets are demodulated and decoded in the receiver according to this information.

If this information regarding physical layer configuration sent after encrypting with a secret key that is known only to valid users, a promiscuous WMAN NIC card not having the key will not be able to decode or demodulate the received data properly. Hence the data available to the hacker will be all junk and it will be very difficult for the hacker to decrypt the data. However, since the number of allowable sets of physical layer configurations in a particular implementation is limited, this scheme only gives limited protection from a hacker who can intelligently generate a possible set of keys which, when used for decryption can cover all the possible sets of physical layer configuration. Hence a second level of protection is necessary. As part of this second level protection, two things can be done. Firstly, some other useful information like length of the packet is also encrypted with the secret key (KEY1). Secondly, the actual data sent subsequently can be encrypted with another time varying key (KEY2), which can be sent as part of the segment encrypted with KEY1. The first process reduces the probability that the hacker will be able to decrypt by intelligently generating a set of keys covering all possible scenarios since now the number of bytes encrypted with the secret key is quite large. The second process provides a second level of security in the sense that even if somehow the physical layer configuration of the receiver is matched to the transmitter, still the data is not recoverable. It also provides a scope of generating a time varying key (KEY2), which allows for added protection.

4 Detailed Description

4.1 Existing Systems

The block diagram of the physical layer of the typical communication system used in Wireless is shown in Figure 1.

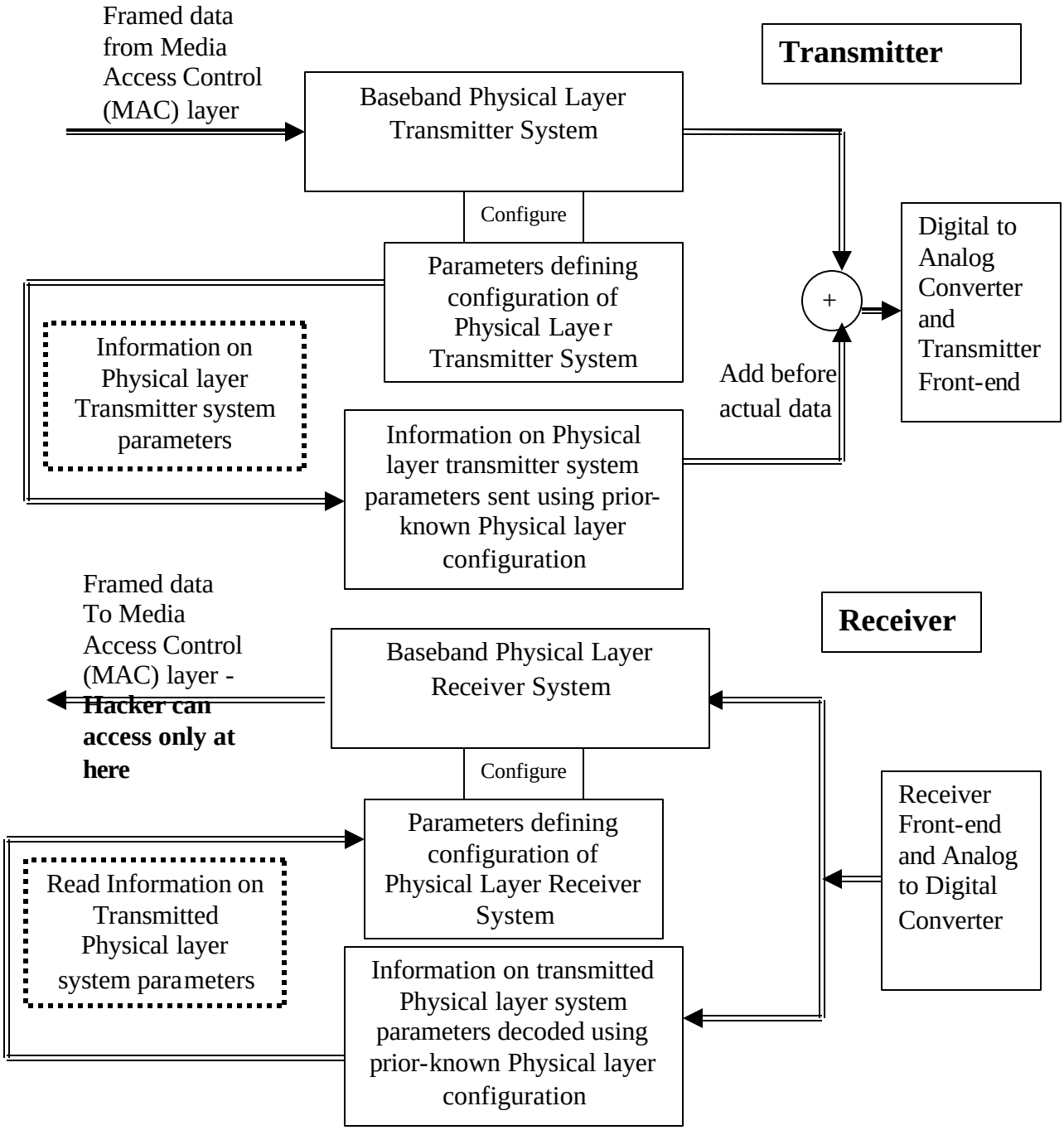

Figure 1 Existing Communication System Block Diagram

4.2 Proposed System

Figure 2 shows where encryption and decryption can be employed to enhance the security (shaded blocks show the new additions)

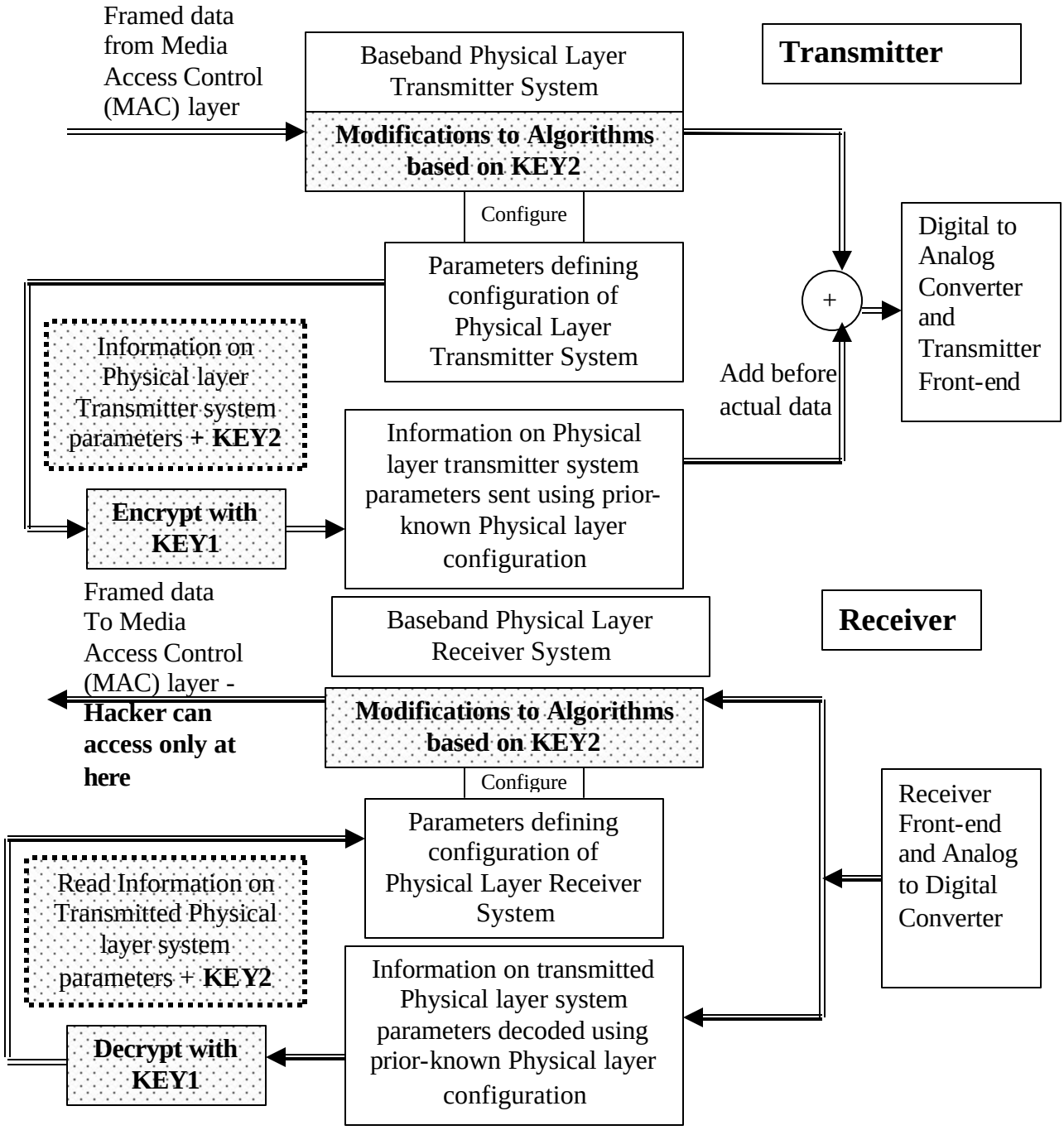

Figure 2 Proposed Communication System Block Diagram

4.2.1 Features

- The first level encryption and decryption are done using the same secret key (KEY1) that is available to all the valid users of the network
- It is assumed that the secret key (KEY1) is delivered to all valid users of the network using some secure mechanism and will be changed from time to time.
- The Physical layer system Parameters encrypted using KEY1 can be
    - Error Control Coding parameters
    - Modulation Type
    - Length of the Packet
    - Scrambling Seed
    - The second level encryption key (KEY2)
    - Any other Information
- Parameters defining different Schemes possible for Error Control Coding can be
    - Type of Error Control Coding (Convolutional, Reed-Solomon, Turbo etc.)
    - Parameter of a particular error control coding (e.g. Rate and Polynomial for Convolutional Code)
- Parameters defining different Schemes possible for Modulation can be
    - Type of Modulation (BPSK, QPSK, QAM etc.)
    - Parameter of a modulation (e.g. constellation for QPSK)
- Parameters that can be modified using KEY2 can be
    - Interleaving pattern
    - Phase offset for OFDM symbols
    - Constellation Mapping
    - Any other information
- A receiver not having the correct key (KEY1) has wrong information about the physical layer system parameters. Hence it cannot configure its Physical layer to proper parameter values required for reception. It also does not know what the second level key is (KEY2).
- A receiver not having the correct KEY2 will not be able to receive the correct data as it will not know the kind of modification that is made in the relevant algorithm parameters. Also the transmitter can change the KEY2 frequently to provide added level of security.

4.2.2 Example

In 802.11g ERP-OFDM, the Physical layer system parameters are modulation technique (BPSK, QPSK, QAM16 or QAM64), convolutional coding rate (1/2, 1/3 or 2/3), packet length and scrambler seed. This information is passed to the receiver through the use of SIGNAL (24 bits) and SERVICE (16 bits) field. The signal field is sent using prior-known modulation (BPSK) and prior-known convolutional coding rate (rate ½).

The following mechanism can be used to enhance the security of the ERP-OFDM system.

- Encrypt SIGNAL field SERVICE field and KEY2 with KEY1 and send to receiver.
- Use KEY2 to modify Physical layer algorithms. The modifications can be -

- The 48 data points of each OFDM symbol input to IFFT can be randomly rotated in phase using random numbers generated from KEY2. The pilot insertion and zero insertion are not phase rotated. This provides an added level of security, as known data is not encrypted.
- Another possible option may be to change the interleaving pattern randomly based on KEY2.

4.2.3 Application to 802.20

The actual PHY to be used in 802.20 is yet to be finalized. But whichever scheme is chosen, the principles described above can always be applied to enhance the security of the system. The security aspects are discussed in details in the next Section.

5 Security Aspects mitigated by proposed scheme

5.1 Data Privacy

Data Privacy is compromised when an unauthorized user gains access to all the encrypted traffic between two points and can decrypt that. To decrypt, one needs the encrypted message, the algorithm and the key. A hacker can discover the key if one is given the encrypted text, the algorithm and the original plain text message. This is commonly known as the "Known Plain-text Attack". Since there is lot of known fields in the header portions, the hacker can run some analyzing software on the recorded encrypted message using some standard Wireless NIC to find out the key and then decrypt the whole message. One suggested way of circumventing this problem is to change the key quite frequently, but it does not provide full-proof security.

In the proposed system, the data recorded by the hacker will be totally wrong because it has been demodulated wrongly, the error control coding rates are different, the constellation demapping is wrong due to random phase shift and the length of the packet is also decoded wrongly. Analyzing such data will not provide any clue to the original key used.

5.2 Data Forgery

Data Forgery happens when an unauthorized user inserts data into network as a valid user. There are two ways valid data enters the network, replay and mimicking. For replaying, the hacker just records the message received and replays it at a latter time. For mimicking, he has to generate some valid messages to mimic some existing valid station.

In the proposed system, since the encryption takes place in the Physical layer, the data itself is not possible to be recorded above MAC layer. Thus replay method is not possible. For mimicking, the hacker needs to have the knowledge of the key. In present systems, the key can be discovered using "Known Plain-text Attack", as described in

section 5.1. Since that is not possible in the proposed system, mimicking also can be prevented.

5.3 Denial of Service

The intruder can flood the network with either valid or invalid messages. The intruder could also jam the channel, inhibiting all transfer of information. This prevents the valid users to use the network service and hence is known as “Denial of Service” attack.

In the proposed system, the hacker can never generate a valid message using software tools. With proper design of the MAC-PHY interface, all invalid messages can be filtered out at the PHY layer itself, thereby limiting the “Denial of Service” effect to minimal damage. However channel jamming cannot be prevented using the proposed system.

6 Summary

In his paper, we have proposed in new technique of encryption in the Physical layer. The very property of the proposed system disallows hackers fom using standard Network Interface cards, recording the data at MAC level, analyzing the recorded data to find out the key and then use the key to decrypt subsequent messages. It also disallows hackers to generate valid messages for Data Forgery and Denial of Service. In the proposed system, even to attempt all such things, the hacker would need costly specialized hardware, which itself will be a big deterrent to hacking.