Channel Dependent Network Layer Encryption

Akash Mukherjee
Senior Undergraduate, Electronics Engineering, IIT(BHU), Varanasi
akash.mukherjee.ece12@iitbhu.ac.in

Abstract: This paper presents a naive idea of making network more robust to quantum attacks. In the upcoming era one of the promising idea is to exploit the properties of wireless channels between the nodes involved in the communication. With the help of channel, we can establish keys for secret communication easily, and that will be random. It will reduce the efforts of communicating the secret key to receivers, as it can be deduced from the channel itself.

Keywords: Cryptography, Network Security, Physical Layer Secrecy, Wireless Channel Characteristics, Key establishment protocols, Data Encryption Standards.

I. Introduction

Digitalization of the world is leading to an increasing demand of information security. Current network layer protocols rely on the computational difficulty of the adversary. With expanding capacity of quantum computers the branch physical layer secrecy is emerging into the scenario of wireless security. This paper proposes a new idea involving fertile use of the characteristics of wireless channel to improve Network Layer Security. Network Security protocols, often known as network encryption applies cryptographic protocols to transmit information to legitimate receivers in presence of eavesdropper, without letting them get hands on the data. In contrast, in the field of physical layer secrecy we exploit the channel characteristics between sender and receiver to provide security. Although, in real time system, to utilize the channel information at the receiver we need to compromise with the data rate a little bit. Because, in mobile communication system the end-to-end path is ever changing, it is not static. So, we need to design a transmit-retransmit system which requires receiver to acknowledge every time it gets a data. There is a trade off. In this paper this fact is considered and its impact has been studied. In other words, current paper offers a complete analysis how the data rate gets affected and also measure how much disagreement is there between receiver and the transmitter. To minimize these undesired effects we can implement sophisticated 'Channel detection techniques at the transmitter' like FEC (Forward Error Correcting Codes), ARQ (Automatic Repeat Request) explained in [i]. Had it been utilized properly, we intend to improve the secrecy by using these channel matrices as keys to secret key protocols, such as DES, AES etc. or in public key cryptography (PKC) in various manner, which is more extensively explained in the next section. A myriad of researches are there for channel estimation and physical layer security by exploiting the so-called curse of communication system, fading, yet to the best of my knowledge, none of these has connected the idea of channel estimation to network protocols to make it more robust to attacks.

Currently, via cryptanalysis a cipher encrypted with Data Encryption Standards can be broken within few weeks at max. And most widely used PKC, RSA; it is reported that around 700 bit RSA cipher can be broken within permissible time. National Security Agency (NSA) is working on quantum cryptography to break any cipher within minutes. With the rise of quantum computers, time is not far when every cipher will be absolutely vulnerable, cracking time will fall drastically [ii]. Our aim is to build an impregnable environment which provides security even in such attacks. Instead of solely believing on computation power limitation of the adversary, we should move on to new mechanism that increase complexity of the computation.

Rest of the paper is organized as follows, Section II explains the current invention in detail, in Section III, the various simulation results are shown to examine it's viability and robustness; and Section IV, concludes with the main idea of the paper.

II. Material and Methodology

Some of the most commonly used physical layer secrecy techniques involves fading of the channel, cooperative jamming. In cooperative jamming, there are some relay nodes between end users which jam signals travelling in-between. This is done in such a manner that signal is indistinguishable for eavesdropper. A very intuitive way is explained in [iii]. Besides, when we use fading to generate secret bits between legitimate pairs, we use the channel characteristics and its time dependance. In the rest of the paper we will consider real time channel characteristics of a fading channel and evaluate its performance to establish a stream of secret bits. In wireless communication,

$y[m] = h[m]x[m] + w[m]$

where,

$y[m]$ = received signal at m-th instant
$x[m]$ = transmitted signal at m-th instant
$h[m]$ = fading characteristics of channel
$w[m]$ = additive white noise

Our invention needs the transmitter to have a prior knowledge about the channel it's transmitting through. A naive way to do this is by sending a pilot career through the channel. Since the characteristics will change soon, so this adds to one of the major drawbacks. To minimize this fallacy, we use modern techniques[i]. Now given the channel characteristics, our aim is to use this to generate secret key for communication in presence of an eavesdropper without letting him any access. One simple implementation can be, we can generate a 64/128 bit secret key (one that is used in DES/AES) by clubbing 'h' over 64/128 coherence time. Coherence time is the time gap where the channel characteristics can be treated as constant. One of the crucial property of a strong key for secret communication protocols is that they should be random, no deterministic relationship between two parts of the key is encouraged. Hence, key generated by our protocol is random as channel characteristics is distributed as a random variable, and we are taking them at a gap of coherence time, i.e. characteristics changes there.

doi : 10.17950/ijer/v5s1/108

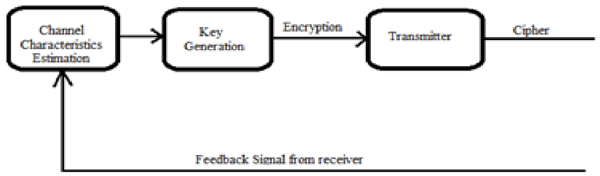

Channel Characteristics Estimation
Key Generation
Encryption
Transmitter
Cipher
Feedback Signal from receiver

Figure: Transmitter side

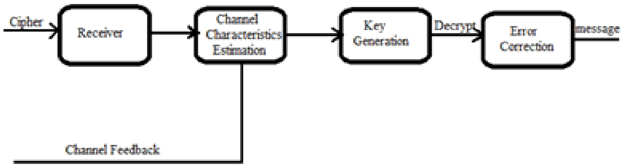


Figure: Receiver side

Another matter of concern is this secret key generation if equally valid for the adversary, provide no intact security. Channel characteristics is different between any two position, but to vary it with significant amount, any of of the receiver or the transmitter should not present near adversary. In that case, he will be able to track every communication perfectly. Current invention deals with this problem very tactically. Knowledge about channel requires a two-way communication, i.e. transmitter sends some signal and receiver acknowledge. We use multipath propagation, transmitter send two copies of signal through to different paths. One straight to receiver and other through trusted third party. To build the key we XOR both of them. Even here a trusted third party is desired, but his knowledge about key is wanting.

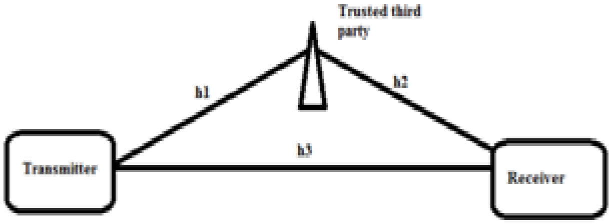


Figure: Communication Model

In this way only the legitimate pair get to know about the channel completely. After each of them receives a fixed number of transmissions, the key is established and secret messaging begins. In case, in-between acknowledge signal is not received transmission is repeated. Once the key is generated successfully, private communication starts, and use the same key for some fixed number of times then reestablish again. This is a notable disadvantage, because in real time environment secret key generation rate of ~0.5 Kbps is very less. Since, we are establishing maximum of 1bit per coherence time.

III. Results and Tables

Here, we are utilizing the random nature of the channel characteristics to establish key between communicators. Although, noise leads to disagreement sometimes. The below plot is a measure to the percentage of error versus SNR.We see the disagreement comes to zero at SNR ~7.5dB.

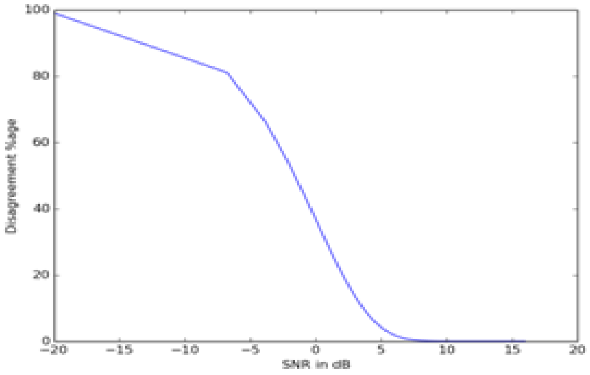
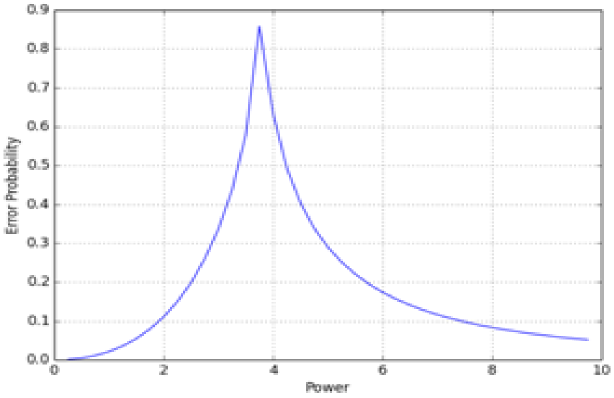


Figure: Disagreement between receiver-transmitter

To analyze the strength of this protocol, we need to present an adversary model. We assume adversary knows the power of the signal, and there is a synchronization between attacker and the user. So, that whenever there is a communication, attacker is able to catch that signal along with some redundant ones. Adversary makes a hypothesis, if 'a' is the power of the transmitting signal, he will only accept signals with power more than that, assuming attenuation to be zero for convenience. If Eve receives a signal S, P(S is a valid signal) > a (Hypothesis)
substituting the PDF, we get the below plot between error and power.



Here we can see the probability is maximum near around 4 in the power axis. We have used 4-QAM, then 64 point OFDM sampling, as OFDM samples tends to behave like gaussian [vi]. Apart from the error due to non-cooperation with the adversary, there are other sources. Hence, even if the adversary is able to detect the correct signal, limited knowledge of pilot career leads to error. Below are two plots where first one is with knowledge of pilot career, and the latter without.

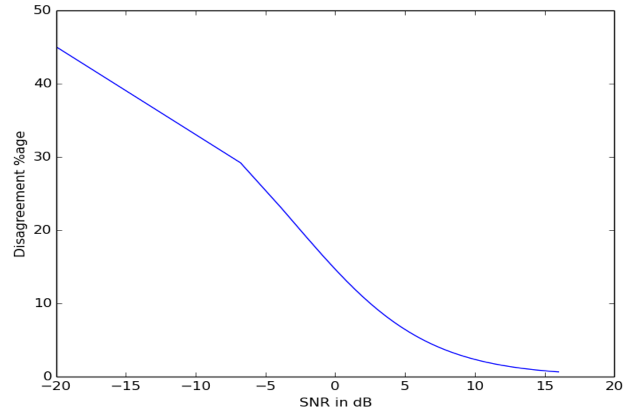


Figure: Disagreement due to no pilot career knowledge

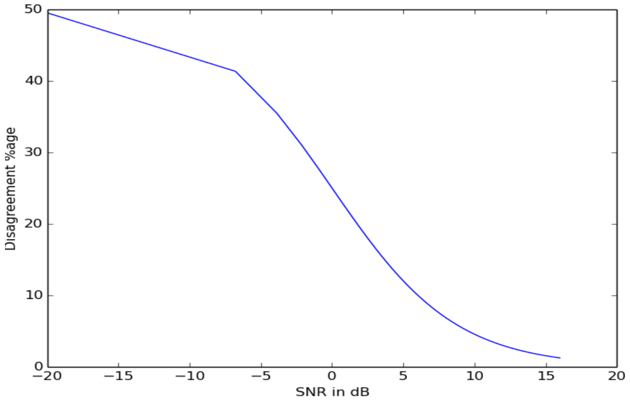


Figure: Disagreement with knowledge of pilot career

Having dealt with error probabilities, let us frame a situation where adversary successfully got every information correct. Present idea provides security in that extreme case also. As we have used multipath propagation, for simplicity we have shown only two, attacker gets knowledge of two out of three channels in the worst case. Resultant is formed using XORing, so the adversary gets no help even after holding that much information.

IV. Conclusion

This paper presents a naive idea of combining physical layer secrecy with network layer to achieve higher security. To evaluate its practicability, we can say it is channel independent after the key agreement is met. In other words, once the key is established, this protocol does not impact the communication speed. So, it is equally applicable for both fast or slow fading channels.

Acknowledgement

I would like to thank everyone surrounding me, without them this would not be possible. First I would like to thank Dr. K. V. Srinivas for sharing his pearls of wisdom during the course of this research. I am immensely grateful to Mr. Aman Soni, Mr. Ankul Gupta for their comments on the earlier version of the manuscript.
Finally, I sincerely thank to my parents, friends for their support and advice.

References

i. S. Šain. Thesis No. 1154. Modelling and Characterization of Wireless Channels in Harsh Environments. MÄLARDALEN UNIVERSITY SCHOOL OF INNOVATION, DESIGN AND ENGINEERING

ii. Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges June 2015 ISBN No. 979-10-92620-03-0 ETSI White Paper No. 8

iii. S. Gollakota, D. Katabi. Physical Layer Wireless Security Made Fast and Channel Independent. MIT. IEEE Infocom 2011

iv. Kluwar Academic Publishers. Data Encryption Standards. Springer US 1997

v. Vincent Rijmen, Joan Daemen. Advanced Encryption Standards. URL: http://www.itl.nist.gov/csrc.nist.gov/publications/fips197/fips-197.pdf. March 1998

vi. R. Van Nee and R. Prasad. OFDM for Wireless Multimedia Communications. Artech House, Inc. 2000

vii. D. Tse and P. Vishwanathan. Fundamentals of Wireless Communications. Cambridge University Press. 2005.

viii. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust Key Generation from Signal Envelopes in Wireless Networks. In CCS, 2007.

ix. A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. CMU.

x. R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," IEEE Tran. on Inform. Forens. Sec., pp. 364–375, Sep. 2007.