

# IOT SECURITY ENHANCEMENT USING PHYSICAL LAYER SIGNATURES

## PROJECT MEMBER'S NAMES:

1. NARAYANAN B – 2016105053
2. VENKAT KRISHNAN B K J – 2016105077
3. ASHOK KUMAR M – 2016105513

GUIDE NAME	SIGNATURE
MRS. N. VIJAYA	

## INTRODUCTION

Wireless networks are susceptible to various attacks due to the “open air” nature of the wireless communication. A secure wireless communication system involves **authentication and secure transmission**. **Authentication** verifies the user identity and prevents malicious users from accessing the network. **Secure transmission** protects data integrity and confidentiality using encryption schemes

Cryptographic key establishment is a fundamental requirement for secure communication to support confidentiality and authentication services. However, it is difficult to ensure availability of a certificate authority or a key management centre in dynamic wireless environments. It is necessary to have alternatives for key agreement between wireless entities in a common channel.

One recent trend in this regard is to use physical-layer signatures. CSI is a fine-grained value derived from the physical layer. It consists of the attenuation and phase shift experienced by each spatial stream on every subcarrier in the frequency domain. CSI provides other attractive properties. First, it is very sensitive to location such that two closely-placed receivers have very different readings by the same sender. Second, its readings of a pair of sender and receiver have a strong correlation. Third, it presents an excellent quality of randomness. Due to these characteristics, CSI is an ideal resource for secret key extraction.

## MOTIVATION

Due to the “open-air” nature, key distribution is more susceptible to attacks in wireless communications. Due to this underlying flaw in the key generation process and the fact that these keys are **less random and predictable**, there are many instances of forced entry on devices protected by these standards. Conventional schemes are based on complex mathematical problems and protocols. These schemes work well for devices having powerful capabilities, such as smartphones. IoT devices are lightweight devices which may not be able to support computationally complex algorithms needed to perform the complex cryptography. This calls for a new key generation method which is less complex, but at the same time secure is necessary to provide better security for such devices.

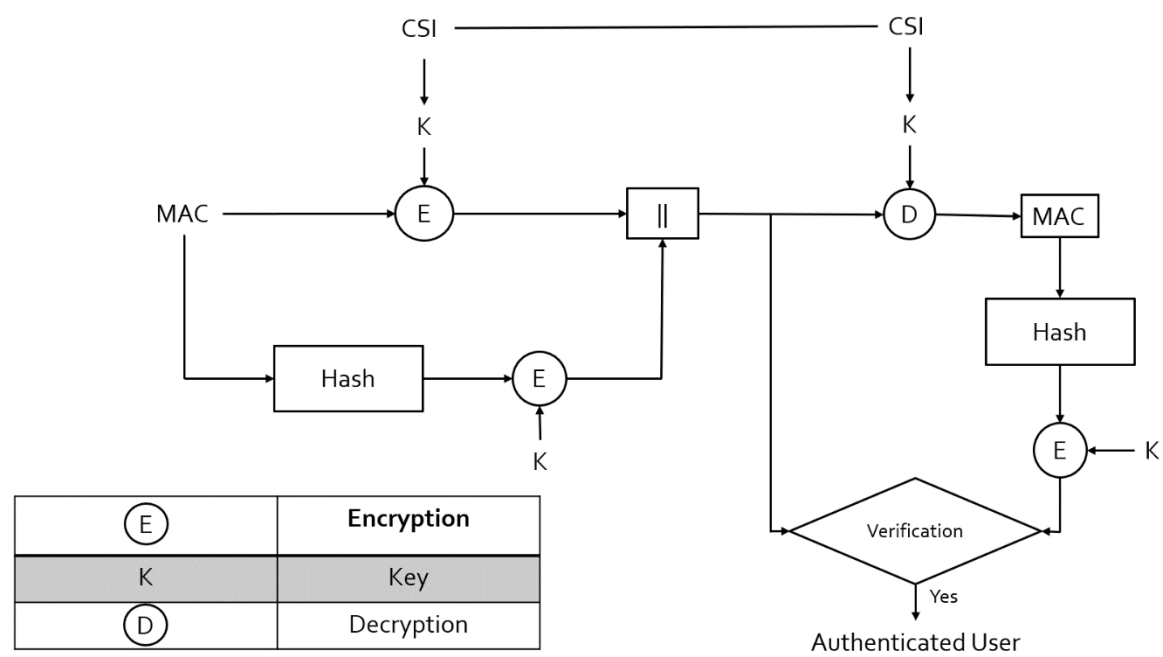
Physical layer security involves physical layer signatures which are very random and doesn't involve complex mathematical computations. These signatures present an excellent quality of randomness and prove to be an ideal resource for secret key extraction.

A new system is proposed where the existing cryptographic securities are enhanced with the incorporation of physical layer signatures

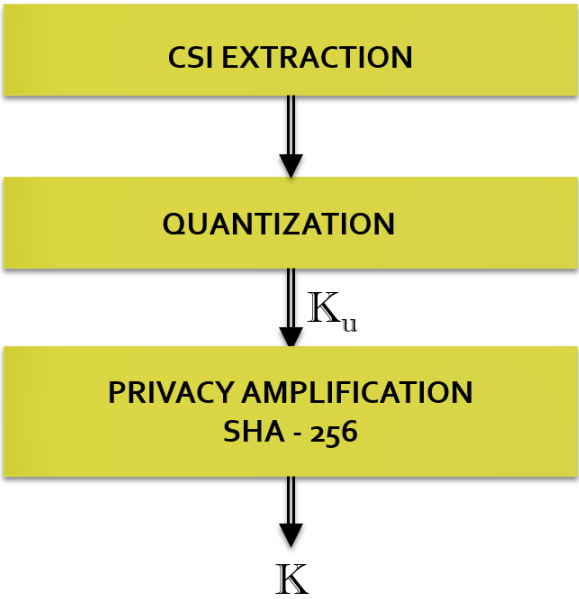
## OBJECTIVE

- To develop a new secret key generation algorithm using physical layer signatures like CSI.
- To overcome key exchange, key distribution and key management overhead at legitimate users.
- To provide significant improvement in secrecy.

METHODOLOGY



KEY GENERATION PROCESS (completed):



## **CSI EXTRACTION**

The CSI values are discarded by the NIC by default which makes it difficult to be used for security purpose in normal devices. However, the Atheros NICs provides a feature by which the CSI values can be read if the kernel of the Linux OS is changed to the supported version. CSI dataset resources are available which can be used for time being. This gives us a set of values describing the channel such as the RSS, Bandwidth, No. of Antennae, CSI in binary format. This binary data must be converted to a suitable readable format and the desired CSI data can be extracted in the form of complex values. The magnitude of the CSI data in different packets are taken and used for quantization.

## **QUANTIZATION**

Cryptographic applications require a binary sequence as the key, but the channel measurements are analog in nature. Quantization can be adopted to convert these analog measurements to digital ones, Ku. The bit-string should be

- Sufficient long, ranging from 128 bits to 512 bits being the length of keys commonly used in symmetric cipher
- Statistically random, resilient to statistical defeats that could be exploited by attackers.

Due to the random nature of CSI, the thresholds needed to quantize the data cannot be fixed in nature. An adaptive-thresholding technique is thus employed to calculate the thresholds keeping in mind that the quantisation thresholds must be tuned to guarantee the same proportion of '0's and '1's, which is an important feature for randomness.

## QUANTIZATION ALGORITHM

INPUT: Absolute value of CSI,  $S$  of length  $N$ ,  $K_d, i = 1 \rightarrow N$

OUTPUT:  $K_u$

Step 1: To find  $\max$  and  $\min$  of  $S$

Step 2: To find quantization threshold by using  $q_t = \frac{\max + \min}{2}$

Step 3: Compare  $S_i$  with  $q_t$

if  $S_i > q_t$  then  $K_d i = 1$

else if  $S_i < q_t$  then  $K_d i = 0$

Step 4:  $\Delta = q_t$

Step 5: while( $\text{no. of zeros in } K_d \neq \text{no. of ones in } K_d$ )

$$\Delta = \frac{\Delta}{2}$$

if  $\text{no. of zeros in } K_d > \frac{N}{2}$

$$q_t = q_t - \Delta$$

if  $\text{no. of ones in } K_d > \frac{N}{2}$

$$q_t = q_t + \Delta$$

Compare  $S_i$  with  $q_t$

if  $S_i > q_t$  then  $K_d i = 1$

else if  $S_i < q_t$  then  $K_d i = 0$



















Step 6:  $K_u = K_d$

## PRIVACY AMPLIFICATION

We use SHA-256 to hash the bit streams, which is highly secure and most widely used of one-way functions. SHA-256 has the following feature: even a small change in the message will, with the overwhelming probability, result in a completely different hash. The CSI input samples are not always of the same length. An added advantage of using SHA-256 is that it always results in a 256-bit message digest which can be used for symmetric encryption

## RESULTS

### Data extracted from NIC

Field 	Value	
 timestamp	3.3446e+09	
 csi_len	140	
 channel	2437	
 err_info	0	
 noise_floor	0	
 Rate	132	
 bandwidth	0	
 num_tones	56	
 nr	1	
 nc	1	
 rssi	14	
 rssi1	14	
 rssi2	128	
 rssi3	41	
 payload_len	1040	
 csi	<i>1x1x56 complex...</i>	
 payload	<i>1040x1 uint8</i>	

### Sample CSI data

```
val(:,:,1) =
```

```
    73.0000 +62.0000i
```

```
val(:,:,2) =
```

```
    72.0000 +70.0000i
```

```
val(:,:,3) =
```

```
    91.0000 +65.0000i
```

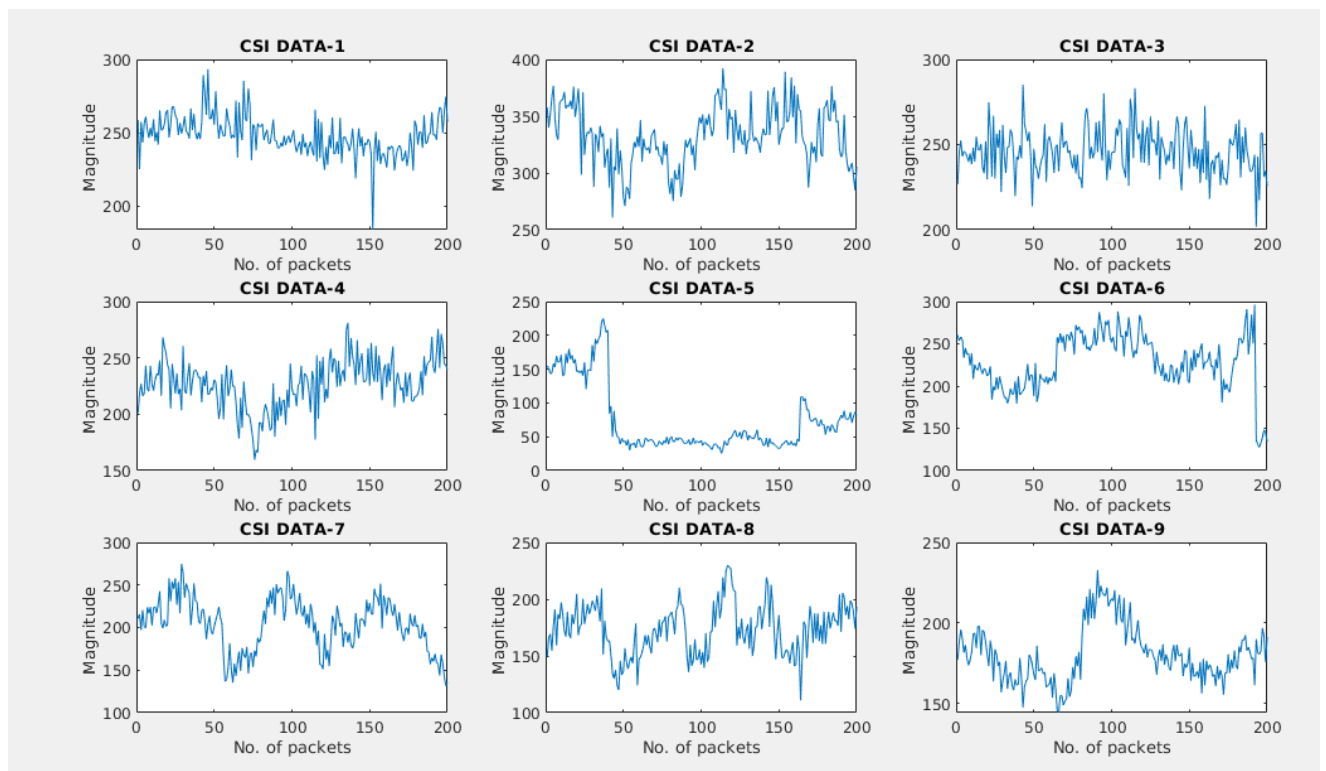
```
val(:,:,4) =
```

```
    90.0000 +47.0000i
```

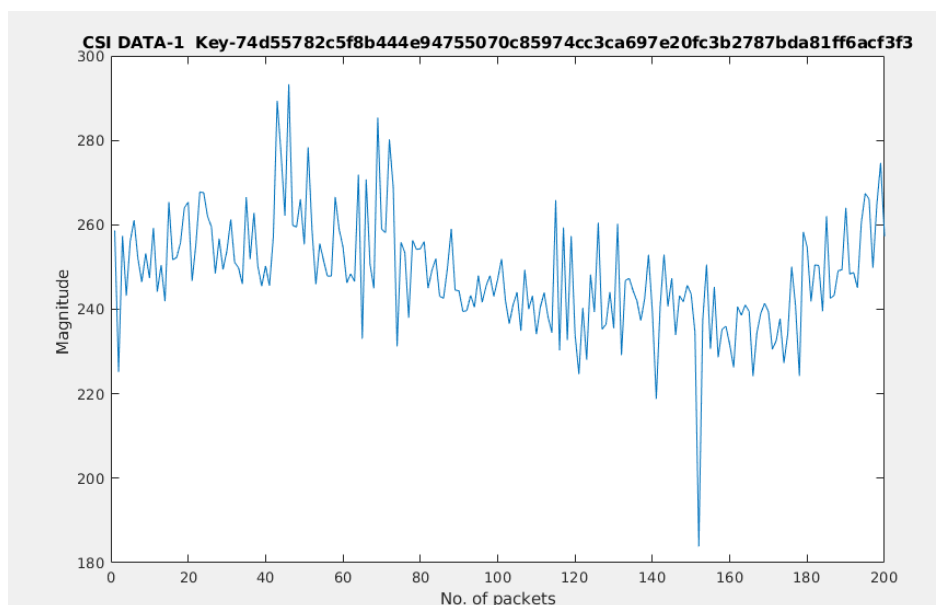
```
val(:,:,5) =
```

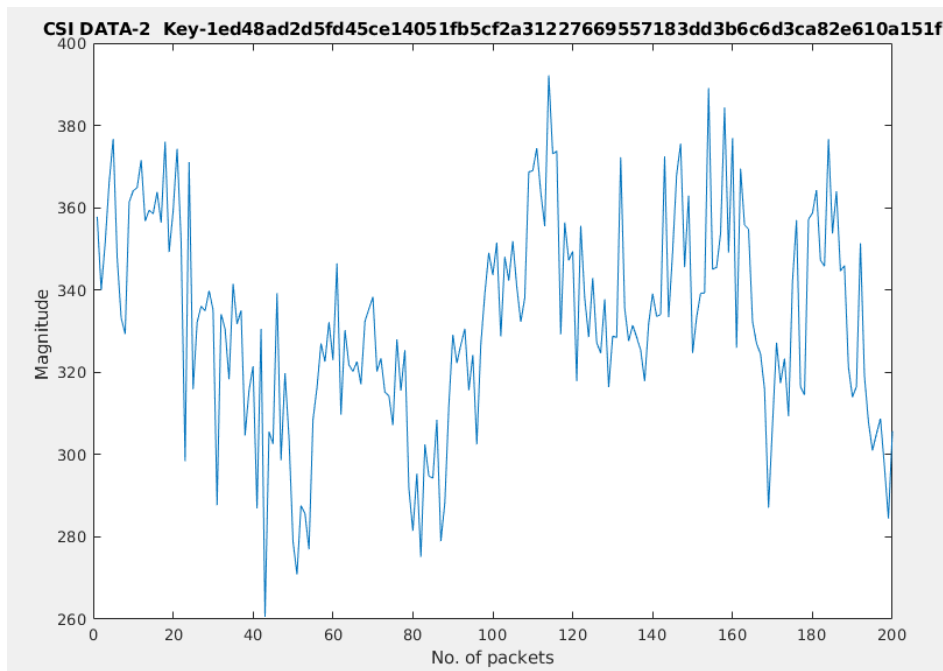
```
    97.0000 +47.0000i
```

## CSI Samples varying with respect to distance and time



## Keys generated for different CSI values





#### TIME FRAME CHART:

	Understanding and Implementation of the proposed key exchange scheme	Implementation and Integration of Authentication protocol with the key exchange scheme.
First Review	Completed	
Second Review		

#### FUTURE WORK:

- Implementation of Authentication protocol using the proposed methodology.
- Integration of Authentication protocol with the key exchange scheme.
- Evaluation of the generated keys using the following performance metrics
  1. Leakage with respect to position
  2. Mismatch Rate



## REFERENCES:

1. **Physical Layer Security for the Internet of Things** by Junqing Zhang, Sekhar Rajendran, Zhi Sun, Member, IEEE, Roger Woods, Senior Member, IEEE, and Lajos Hanzo, Fellow, IEEE. Published in: IEEE Wireless Communications (Volume:26, Issue: 5, October 2019)
2. **Key Generation From Wireless Channels: A Review** by Junqing Zhang, Trung Q. Duong, (Senior Member, IEEE), Alan Marshall, (Senior Member, IEEE), and Roger Woods, (Senior Member, IEEE) 2016. Published in: IEEE Access (Vol. 4)
3. **Wireless Physical Layer Identification : Modeling and Validation**, by W.Wang, Z.Sun, S. Piao, B. Zhu, and K. Ren, IEEE Trans. Inf. Forensics Security, vol. 11, no. 9, pp. 2091–2106, 2016
4. **Efficient and Secure Key Extraction using CSI without Chasing down Errors**  
Jizhong Zhao, Wei Xi, Jinsong Han, Shaojie Tang, Xiangyang Li, Yunhao Liu, Yihong Gong, Zehua Zhou