Volume 6, Issue 11, November 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

www.ijarcsse.com

Research Paper

Available online at: www.ijarcsse.com

# Simulation of Secure Communication Using Decoy State Enabled Quantum Key Distribution in Computer Networks

**K Sai Prabanjan Kumar**
M.Tech & JNTUA,
India

**C. Raghavendra**
CSE & JNTUA,
India

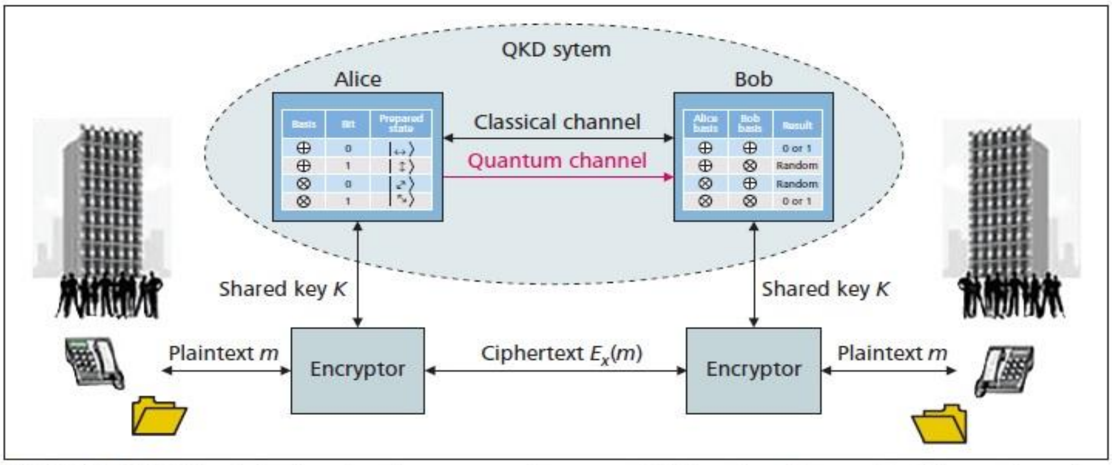
**Dr. A. Kumaravel**
CSE & Bharath University,
India

***Abstract— Quantum key distribution is an innovative technology that exploits the laws of quantum mechanics to generate and distribute unconditionally secure shared key for use in cryptographic applications. However, QKD is a relatively nascent technology where real world system implementation differ significantly from their ideal theoretical representations. A modeling approach is built upon the Object oriented programming based discrete event simulator that can study the impact of implementation non idealities on QKD system performance and security .It is usefull in studying the device imperfections and practical engineering imitations through the modeling and simulation of polarization based, prepare and measure BB84 QKD reference architecture. The performance of a QKD system against a modeled photon number splitting attack is analysed, where if a pulse generated by ALICE contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. An improvement in performance can be achieved using the decoy state enabled BB84 protocol and its immunity to the photon number splitting attack is demonstrated .***

***Keywords— Quantum Key Distribution, Modeling & Simulation, Photon number splitting attack , OMNeT++, BB84 protocol.***

## I. INTRODUCTION

Quantum Key Distribution (QKD) is used for providing secure communication between two communicating parties.Quantum key distribution (QKD) enables two communicating parties to share a random bit string known only to them, which is known only to them by removing the parts of the intercepted bit string ant thus forming a one-time pad. Its secrecy is founded on the laws of nature, as opposed to the computational complexity assumptions used in conventional cryptography.It enables the sender and the receiver to produce a random bit string known only to them,which can be use as a key to encrpt and decrpt messages. The unique property of the Quantum key distribution is in enabling the sender and receiver in identifying the third party interference in the channel that is trying to gain the knowledge of the key unauthorised. This is achieved by the usage of qubits by the Quantum Key Distribution in sending information from the sender to receiver, which will change their state when copied or its value is measured. However, the change in state of a qubit can also occur by the environment and cannot be distinguished from the modification caused by an unauthorised third party. Thus, any disturbance of the quantum signal produced in the communication channel destroys the performance of a QKD system. Quantum signals are delicate in nature and can be destroyed even by the smallest interferences. The traditional solution to this problem has been to use a dedicated fiber for the quantum channel: the part of a QKD system that carries the single quantum signals. But, it is economically unviable.



| Basis | Bit | Prepared state |
|---|---|---|
| ⊕ | 0 | $\lvert\leftrightarrow\rangle$ |
| ⊕ | 1 | $\lvert\updownarrow\rangle$ |
| ⊗ | 0 | $\lvert\nearrow\rangle$ |
| ⊗ | 1 | $\lvert\searrow\rangle$ |

| Alice basis | Bob basis | Result |
|---|---|---|
| ⊕ | ⊕ | 0 or 1 |
| ⊕ | ⊗ | Random |
| ⊗ | ⊕ | Random |
| ⊗ | ⊗ | 0 or 1 |

Figure 1. A BB84 polarization-based prepare and measure QKD system. The sender Alice and receiver Bob are configured to generate a shared secret key for use in bulk encryptors, where the quantum channel (i.e., a freespace or optical fiber link) is used to securely transmit qubits, and the classical channel is used to facilitate the BB84 protocol.

## II. RELATED WORK

Object oriented programming techniques are used for building network modules in the OMNeT++ Integrated Development Environment (IDE) . Eclipse platform is used by the simulator for performing it's operations on the c++ based network modules. UML modelling , bug tracker integration, database access, integrated SVN/GITrotocols, editing c++ code ,etc:-will be provided support by the eclipse platform for the OMNeT++ .Network simulations in OMNeT++ can be performed on wired or wireless communication networks ,on- chip networks ,etc:-. NED (Network Description Language) is an important component in the OMNeT++ simulator ,that can be operated in both graphical mode and in text mod. Graphical mode can be used for creating compound modules ,channels and other component types. NED is a high level language that can be used for assembling components of a simulated network that are written in c++. OMNeT++ is usefull in distributed component architecture development for network based models. Component based architecture development of OMNeT++ ensures reusability of the components.

## III. EXISTING SYSTEM

A BB84 algorithm:

The protocol is divided into three phases

1> Preparation phase (Alice)

2> Preparation phase of key (Bob)

3> KEY Measurement and derivation phase ( Alice)

Preparation phase:

ALICE sends a random sequence of photons, |v> - photon (0 degrees) , |h> - photon (90 degrees) ,|lcp> - photon (45 degrees) , |rcp> - photon (135 degrees).

Preparation of key phase:

BOB randomly chooses his detector basis from R – basis or D – basis to easure each photon . BOB reports his detector bases for each photon.

KEY Measurement and derivation phase:

ALICE tells BOB which bases were correct .Finally ALICE and BOB will share the bits where ALICE response is TRUE or MATCHED and discards all other bits .Parity bits or error correcting bits can also be added through the public channel to ensure that the key is error free.

But the existing system is susceptible to various attacks like Photo Number Splitting (PNS) attack. Alice sends photons to Bob for key generation phase to initiate in the BB84 protocol. This, can be performed in practise by using laser pulses' magnitude being reduced to very low level, so that more than single photon will never be generated . Laser pulses with such very low magnitude contain further small number of photons, if 0.2 photons are considered to be present in each pulse , in practise only a poission distributuion of that value exists in each signal. Poission distribution makes some photons contain no photons,(i.e, even after such a pulse is received no photons will be present in them ) .Some pulses contain an ideal single photon scenario,where,such signals carry one photon. Some pulses contain an ideal single photon scenario, where,such signals carry exactly one photon. Some pulses contain 2 or more photons which makes the PNS attack scenario a possibility .The signals or the pulses in which more than one photon is present ,Eve can take away and store the extra photon from the signal and transmit the rest of the photons to Bob. This is very important step in PNS attack , as Eve keeps the extra photons in quantum memory.

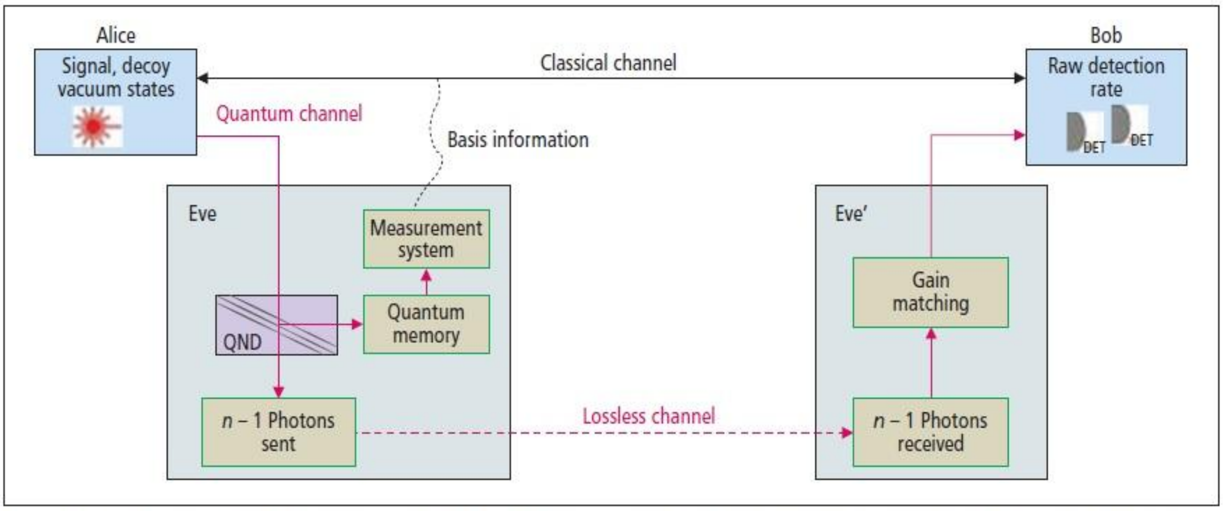
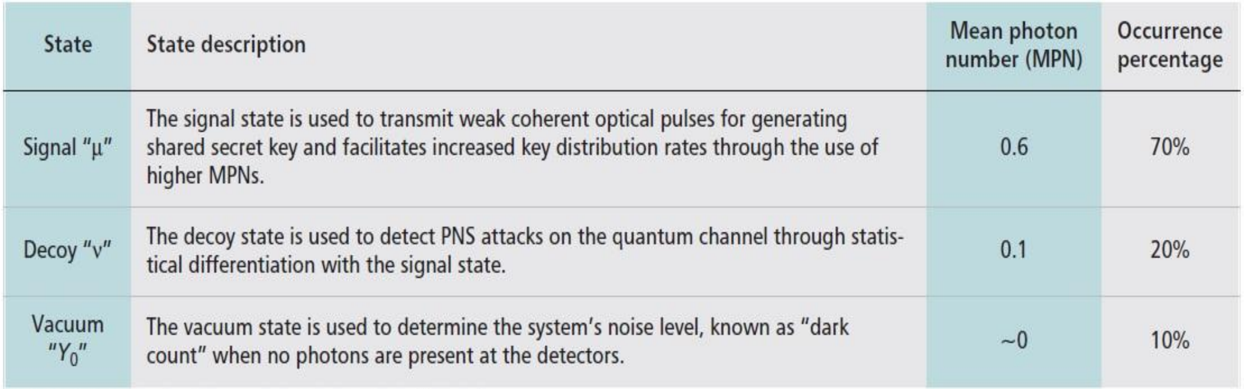


Figure 2. A generalized depiction of Eve's photon number splitting attack conducted against Alice's and Bob's decoy state enabled QKD system.

## IV. PROPOSED SYSTEM

The Alice randomly sends some of the laser pulses with a lower average photon number as decoy states. These decoy states can be used to detect a PNS attack, as Eve can not tell which pulses are signals and which are decoy. Using this idea the secure key rate scales as, the same as for a the scenario with single photon emitting source.



| State | State description | Mean photon number (MPN) | Occurrence percentage |
|---|---|---|---|
| Signal "μ" | The signal state is used to transmit weak coherent optical pulses for generating shared secret key and facilitates increased key distribution rates through the use of higher MPNs. | 0.6 | 70% |
| Decoy "ν" | The decoy state is used to detect PNS attacks on the quantum channel through statistical differentiation with the signal state. | 0.1 | 20% |
| Vacuum "$Y_0$" | The vacuum state is used to determine the system's noise level, known as "dark count" when no photons are present at the detectors. | ~0 | 10% |

**Table 1.** Example decoy state protocol configuration.

### 4.1 Efficiency Based Security Condition

A more precise variation of the decoy state security condition that allows PNS attacks to be detected without a priori knowledge of the quantum channel efficiency. This approach is particularly advantageous as it is nearly impossible to guarantee a known secure state of the quantum channel over many kilometers. Similarly, it is difficult to ensure secure system performance. During operation of decoy state enabled systems, the signal and decoy state yields are estimated from the measured gains Qsignal, Qdecoy, and the dark count rate $Y_O$.

$$Q^{\text{signal}} = \frac{\text{Number of detections during signal pulses}}{\textit{Total number of signal pulses sent}}.$$

$$Q^{\text{decoy}} = \frac{\text{Number of detections during decoy pulses}}{\text{Total number of decoy pulses sent}}.$$

$$Y_0 = \frac{\text{Number of detections during vacuum pulses}}{\text{Total number of vacuum pulses sent}}.$$

The gain Q is the product of the probability of Alice sending out an n-photon pulse (a Poisson distribution) and the conditional probability of Alice's n-photon pulse leading to a detection event at Bob (Yn). where m is the signal MPN (or v is the decoy MPN), n is the number of photons in each pulse leaving Alice, $Y_0$ is the dark count rate, which is typically characterized during calibration activities, and h is the system's measured quantum efficiency,including the quantum channel, Bob's optical components, and Bob's detector efficiency.

where signal and decoy efficiencies can be directly calculated and compared from the measured gains Qsignal, Qdecoy. We also realize that due to non-ideal devices and probabilistic single photon sources, we expect variations D in the calculated efficiency and the security condition becomes

$$h^{\text{signal}} = h^{\text{decoy}} \pm D.$$

The proposed secure condition should always be true unless a PNS attack is occurring.
In contrast, $h^{\text{signal}} = h^{\text{decoy}} \pm D$. implies eavesdropping on the quantum channel.

## V. CONCLUSIONS

In this paper the function of BB84 Quantum Key distribution Protocol with the existence of eavesdropper and a model-based technique for security analysis of it is provided . When Eve conducts PNS attacks, the signal state efficiency remains relatively unchanged, while the decoy state efficiency drops considerably. This is primarily due to the difference in MPNs, where Eve blocks a majority of the lower MPN decoy state pulses and must send slightly more signal state pulses in order to meet Bob's expected detection rate. Figure 4 depicts the signal and decoy efficiencies under normal operating conditions and the resulting efficiencies when Eve is conducting a PNS attack. The overlapping signal and decoy efficiencies (i.e., within the 99.9 per cent security tolerances) imply hsignal = hdecoy and indicate secure operation. This simulation study illustrates how the efficiency-based decoy state security condition can be used to easily and accurately detect PNS attacks without assuming a known secure quantum channel. As indicated by the relatively large difference between the PNS induced decoy state efficiency and the normal efficiencies, Eve's PNS attack is readily detectable when properly configured.

## REFERENCES

[1] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, ''Performance evaluations of quantum key distribution system architectures,'' IEEE Security Privacy, vol. 13, no. 1, pp. 30–40, 2015.

[2] N. T. Sorensen and M. R. Grimaila, ''Discrete event simulation of the quantum channel within a quantum key distribution system,'' J. Defense Model. Simul., Appl., Methodol., Technol., 2015.

[3] K. Passive Decoy-State Quantum Key Distribution with Coherent Light MarcosCurty 1, *, Marc Jofre 2.doi:10.3390/e17064064.

## AUTHORS PROFILE

**K. Sai Prabanjan Kumar** received B.Tech degree in Computer Science Engineering from Jawaharlal Nehru Technological University college of engineering ,Pulivendula affiliated to JNTUA College of Engineering, Ananthapuramu, A.P,India, during 2009 to2013. Currently pursuing M.Tech in Computer Science at JNTUA College of Engineering, Ananthapuramu,A.P, India, during 2014 to 2016. His area of interest is Algorithms and Data structures.

**Mr. C. Raghavendra** is a scholar in Bharath University, Chennai and working as a Lecturer in Computer Science and Engineering department in Jawaharlal Nehru Technological University College of Engineering, Ananthapuramu. He obtained his Bachelor degree in Computer Science & Information Technology from JNTUH, Master of Technology in Computer Science from Bharath University, Chennai and pursuing Ph.D. in Bharath University, Chennai. He has published several Research papers in National and International Conferences and Journals. His areas of interests are Networks andImageprocessing.

**Dr. A. Kumaravel** Working as a professor in CS for more than 20 years in Singapore, Dubai and Malaysia. Currently is working as Dean for School of Computing. He has published many research papers, and he also presented numerous papers in national and international conferences. His areas of interests are Distributed Computing, Learning Machines, Software Engineering and theory of Programming Languages.