International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 935-938 www.ijaem.net ISSN: 2395-5252

Asymptotic Estimation for Hybrid Massive MIMO Channel Communication Evolution

Dr.J.ARUN, M.E., Ph.D.,[1] Head of The department, J. Prabhakaran,[2] A.Raja,[3] S.Suresh,[4] T.Veeramani [5]

Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur.

Submitted: 05-05-2021 Revised: 17-05-2021 Accepted: 20-05-2021

ABSTRACT: The Physical-layer key generation (PKG) based on channel reciprocity establish secret keys between devices. The fifth generation (5G) wireless communications employ massive multiple-input multiple-output (MIMO) to, support multiple users simultaneously. It presents a multi-user secret key, generation in massive MIMO wireless networks. This channel model analyze, the secret key rate and derive a closed-form expression under independent channel conditions. The proposed optimization design can significantly reduce the pilot overhead of the reciprocal channel state information acquisition. The channel gains from different transmit directions to different receive directions. To maximize the sum secret key rate, provide the optimal conditions for the Kronecker product of the precoding and receiving matrices and propose an algorithm to generate these matrices with pilot reuse. The proposed optimization design can significantly reduce the pilot overhead of the reciprocal channel state information acquisition.

I. INTRODUCTION

Introduction to Peer-to-Peer Network: Human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications Mobile computing is "taking a computer and all necessary files and software out into the field." "Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing." "Mobile computing is the ability to use computing capability without a pre-defined location and/or connection to a network to publish and/or subscribe to information."

Peer-to-peer (p2p) networks, such as Napster, Gnutella, and BitTorrent, have become essential media for information dissemination and sharing over the Internet. Concerns about privacy, however, have grown with the rapid development of P2P systems. In distributed and decentralized P2P environments, the individual users cannot rely on a trusted and centralized authority, for example, a Certificate Authority (CA) center, for protecting their privacy. Without such trustworthy entities, the P2P users have to hide their identities and behaviors by themselves.

Routing and resource discovery: Peer-to-peer networks generally implement some form of virtual overlay network on top of the physical network topology, where the nodes in the overlay form a subset of the nodes in the physical network. Data is still exchanged directly over the underlying TCP/IP network, but at the application layer peers are able to communicate with each other directly, via the logical overlay links (each of which corresponds to a path through the underlying physical network). Overlays are used for indexing and peer discovery, and make the P2P system independent from the physical network topology. Based on how the nodes are linked to each other within the overlay network, and how resources are indexed and located, we can classify networks as unstructured or structured (or as a hybrid between the two).

II. REVIEW OF LITERATURE

2.1 Secret Key Generation Exploiting Channel Characteristics In Wireles Communications (Kui Ren, Hai Su, And Qian Wang)

Abstract

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community. However, the development of such a mechanism requires a comprehensive understanding of the problem and the techniques that have been used thus far in preventing, detecting, and responding to various DDoS flooding attacks.

In this paper, we explore the scope of the DDoS flooding attack problem and attempts to combat it. We categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, we highlight the need for a comprehensive distributed and collaborative defense approach. Our primary intention for this work is to stimulate the research community into developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack.

2.2 Secret Key Generation from Sparse Wireless Channels: Ergodic Capacity and Secrecy Outage(Tzu-Han Chou, Stark C. Draper, Akbar M. Sayeed)

Abstract

With the exponential growth of the Internet use, the impact of cyber-attacks are growing rapidly. Distributed Denial of Service (DDoS) attacks are the most common but damaging type of cyber-attacks. Among them SYN Flood attack is the most common type. Existing DDoS defense strategies are encountering obstacles due to their high cost and low flexibility. The emerging of Network Function Virtualization (NFV) technology introduces new opportunities for low- cost and flexible DDoS defense solutions. In this work, we propose CoFence a DDoS defense mechanism which facilitates a collaboration framework among NFV-based peer domain networks. CoFence allows domain networks help each other's handle large volumes of DDoS attacks through resource sharing. Specifically, we focus on the resource allocation problem in the collaboration framework. Through CoFence a domain network decides the amount of resource to share with other peers based on a reciprocal-based utility function. Our simulation results demonstrate the designed resource allocation system is effective, incentive compatible, fair, and reciprocal.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

- The measurements of the uplink and downlink channel are not identical but highly correlated.
- The key distribution is usually handled by the traditional public key cryptography techniques.
- The distributed key for each device usually does not update for a long time which may incur security issues.
- However, the channel varies slowly such that the adjacent measurements are highly correlated, which will introduce redundancy and may finally result in failure of key generation.

Demerits

- Multi-user secret communications are very demanding.
- Multiple users participating in the key generation process.
- The majority of them still perform channel probing in a pairwise manner, resulting in an extremely large overhead and low efficiency.

PROPOSED SYSTEM

- The PKG process generally contains four stages, namely channel probing, quantization, information reconciliation, and privacy amplification.
- Based on channel reciprocity, the channel probing stage shares the common random sources between legitimate users to generate the secret keys.
- MIMO systems, it is impractical for the base station (BS) and the user terminal (UT) to estimate the instantaneous uplink and downlink channel information within the coherence time.
- Channel Dimensionality Reduction(CDR)-based key generation scheme exploiting sparse property of the beam domain channel Model.

Advantages

- A multi-user secret key generation framework and provide a general secret key rate, containing both cases.
- BS allocates non-overlapping beams to different UTs and multiple UTs can simultaneously generate secret keys with the BS using non-overlapping beams.
- Multi-user key generation yet receives less attention.

IV. SYSTEM DESIGN

It is a process of planning a new business system or replacing an existing system by defining its components or modules to satisfy the specific requirements. Before planning, you need to understand the old system thoroughly and determine how computers can best be used in order to operate efficiently. System Design focuses on how to accomplish the objective of the system.

DATA FLOW DIAGRAM

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system. A data-flow diagram (DFD) is a graphical representation of the “flow” of data through an information system. Figure 5.2 is show the process of data uploading and downloading.

Authentication: The basic feature of this method is to allow the user to anonyms’ authentication to access the files and document served in the server and then tracks the ownership and identity of the user. The system consists of a single attribute. The user gets two keys after register into the system. For the decryption attribute key will be used by the further user to preserve the security & traceability of the user the encrypted user need to sign the data using a group signature key.

V. SYSTEM DESIGNING

Data Sharing

The Hybrid environment consists of two or more public private environment connected together. Each environment has their own security policy so the privacy of the data is very important. For data sharing in a hybrid environment a common data center is used to manage all the data through this data can be shared among the different user. In the health care industry all hospitals, research, development centers all connected together to form a hybrid environment. The user needs to access the data of another need to send requests to the common data center. By the laws of HABE algorithm, any eavesdropper (Eve) that snoops on the quantum channel will cause a measurable disturbance to the flow of single photons.

Secret Key Generation

Users first obtain multi-attribute-based keys from their data owner. They submit their identity information and obtain secret keys that bind them to claimed attributes. For example, a user would receive as her attributes, possibly from different data owner. In addition, the data owners distribute write keys that permit users in their write to some records. A user needs to present the write keys in order to gain write access to the server.

Beam Domain Transform

Beam domain transform samples the original physical channel by two series of uniformly distributed beams/angles over transmitting and receiving beams/angles. Firstly, in the beam domain, the channel matrix reveals the sparse property, i.e., only a few elements contain the most channel information, which reduces the dimension of channel estimation. Secondly, as the number of antennas at the BS and UT increases, the elements of the channel matrix become mutually independent, reducing the redundancy, which is particularly desirable in secret key generation.

Compound Classification

The compound classification on the correlated flows modelled by a bag-of- flows (BoF) instead of classifying individual traffic flows. All flows sharing the same 3-tuple are generated by the same application and should belong to the same traffic class. The correlation information can be utilized to improve the classification accuracy.

VI. SOFTWARE SPECIFICATION

GENERAL This chapter is about the software language and the tools used in the development of the project. The platform used here is J2EE. The Primary languages are JAVA and MYSQL.

THE JAVA PLATFORM

6.1 Java

Java acts as the front end, which drives its syntax from C and object-oriented features from C++. The main feature is platform independent. Java is popular among Internet programmers. It expends the universe of objects that can move about freely in cyberspace. Java can be used to create two types of programs, application and applets. An application is a program that runs on the computer, under the operation system of that computer. An applet is a tiny java program, dynamically downloaded across the network.

6.2 The Byte code

The output of java compiler is not executable code, it is byte code. It is a set of instructions to be executed by java run-time system called java virtual machine (JVM) it is an interpreter for byte code.

VII. TESTING

7.1 GENERAL

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product it is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product it is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

VIII. CONCLUSION

This project provided a fundamental design and analysis of the multi-user secret key generation in massive MIMO wireless networks. This provided a beam domain channel model, representing the channel gains from different transmit directions to different receive directions. We derived a closed-form expression of the secret key rate, which depends on the statistical CSI and the precoding and receiving matrices. This provided the optimal conditions for the Kronecker of the precoding the receiving matrices and proposed an algorithm to achieve the maximal sum secret key rate. When the beams of different UTs are non- overlapping, the BS employs several strongest beams of each UT to simultaneously generate secret key.

IX. FUTURE WORK

Furthermore, provided a security analysis by considering the channel correlation between UTs. When the channels of different UTs are correlated, the BS employs the several strongest non-overlapping beams of each UT to generate secret key. Numerical results demonstrate the performance improvement of our proposed multi-user secret key generation scheme. This work focuses on the sum secret key rate maximization, while the power allocation optimization under the fairness constraint among UTs can be further analyzed in the future.

REFERENCES

[1] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, “Key generation from wireless channels: A review,” IEEE Access, vol. 4, pp. 614–626, Mar. 2016.

[2] C. Chen and M. A. Jensen, “Secret key establishment using temporally and spatially correlated wireless channel coefficients,” IEEE Trans. Mobile Comput., vol. 10, no. 2, pp. 205–215, Feb. 2011.

[3] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, “High-agreement uncorrelated secret key generation based on principal component analysis preprocessing,” IEEE Trans. Commun., vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[4] J. Zhang, T. Duong, R. Woods, and A. Marshall, “Securing wireless communications of the Internet of Things from the physical layer, an overview,” Entropy, vol. 19, no. 8, p. 420, Aug. 2017.

[5] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, “Securing the Internet of Things in a quantum world,” IEEE Commun. Mag., vol. 55, no. 2, pp. 116–120, Feb. 2017.

[6] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, “Information reconciliation schemes in physical-layer security: A survey,” Comput. Netw., vol. 109, pp. 84–104, Nov. 2016.

[7] E. A. Jorswieck, A. Wolf, and S. Engelmann, “Secret key generation from reciprocal spatially correlated MIMO channels,” in Proc. IEEE Globecom Workshops (GC Wkshps), Atlanta, GA, USA, Dec. 2013, pp. 1–6.