International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SECURE DATA TRANSMISSION USING BLOCK CHAIN WITH SHA

K. RANJITH REDDY[1], SP. SATHWIKA[2], S. KALYANI[3], U. SHIVANI [4]

[1]Assistant Professor, Department of ECE, Mallareddy Engineering College For Women

[2,3,4]UG Scholar, Department of ECE, Mallareddy Engineering College For Women

ABSTRACT

Internet of Things (IoTs) is an integrated network collection of heterogeneous objects which enable seamless integration between systems, humans, devices, and various other things, to support pervasive computing for smart systems. IoT-driven systems and sensors continuously ingest data resulting in an increased volume and velocity of information which can lead to critical concerns such as security of the data and scalability of the system. The Internet of Underwater Things (IoUTs) is a specific genre of IoTs in which data related to oceanic ecosystems is continuously sensed through underwater sensors. IoUT has emerged as an innovative paradigm to support smart oceans. However, there are several critical challenges which IoUT system designers must consider such as (i) scalability of the system to handle large volumes of oceanic data and (ii) security of data that is transmitted from IoT sensors deployed underwater. Blockchain as a newly emerged technology and an enabling platform allows decentralized and secure transmission of data among a wide group of untrustworthy parties. This research aims to exploit blockchain technology to secure IoUT data transmission by exploiting Interplanetary File System (IPFS) method. Additionally, this study also addresses the system's scalability in two aspects, (i) scalability, and (ii) security. We used a case study-based approach and performed experiments to evaluate the proposed solution's usability and efficiency in terms of query response (i.e., performance), and algorithmic execution (i.e., efficiency). The proposed solution unifies blockchain technologies to secure IoT-driven systems and provides guidelines to engineer and develop next-generation of robust and secure blockchain-aided distributed IoT systems.

INTRODUCTION

COMMUNICATION with chaos has attracted significant interest in the literatures [1], [2], [3], [4] since early 1990s. In recent years, more properties of chaos have been reported to be fit for wireless communication applications, such as the Lyapunov spectrum invariance property of chaotic signal after transmitted through wireless channel [5]. Chaos is proven to be the optimal communication waveform in the sense of very simple matched filter being used to achieve the maximum signal to noise ratio (SNR) [6]; the chaotic baseband waveform generated by the chaotic shape-forming filter (CSF) is proven to be topologically conjugate to the symbolic sequence [7], which means that arbitrary information sequence can be encoded into the chaotic waveform; the intersymbol interference (ISI) caused by multipath propagation can be eliminated in theory by using the proper decoding threshold [8], and the chaotic waveform can be used as the baseband signal under the conventional wireless communication system framework, in order to improve the bit error rate (BER) performance with the simpler and lower cost algorithm [9]. However, the distortion of wireless channel

transmission in outdoor environment significantly degrades the performance of both the conventional wireless communication system and chaotic wireless communication system. A good channel estimation helps improving the BER performance, and making the communication system reliable. For this purpose, it is generally required to transmit a pilot sequence in the conventional estimation methods, such as the classical least squared (LS) approach, minimum mean squared error (MMSE) algorithm [10] and so on. On one hand, the conventional methods always need the pilot (training) sequence sent before the data sequence, which consumes the valuable bandwidth and reduces the data transmission rate. On the other hand, the conventional channel estimation methods are generally suffering from performance degradation due to the serious environment noise. To deal with these challenges, the autocorrelation function (ACF) property of the chaotic signal is exploited in [11], and it is used to identify the channel parameters without any pilot sequence, which improves the channel identification performance effectively. However, the blind channel identification based on ACF of chaotic signal is a complicated process by resolving a mathematical nonlinear problem. Thus, a novel solution is expected to avoid solving the complicated nonlinear equation. Due to the excellent generalization ability and powerful learning capacity of deep learning (DL) [12], it is opening up new way for the problems that are difficult to be solved by conventional methods in wireless communication [13], [14], as well as in chaotic wireless communication [15], [16], [17]. There have been many interesting results about using DL for the physical layer, including channel estimation [18], signal detection [19], etc. Among the DL applications to wireless communication systems, channel estimation is one of the most widely studied issues. Recently, the DL estimator has emerged as a promising alternative to address channel estimation problem in wireless communication systems [20] and shown excellent performance. The first attempt has been made in [21] to learn the characteristics of frequency selective wireless channels and combat the nonlinear distortion and interference for orthogonal frequency division multiplexing (OFDM) systems by applying the powerful DL methods. In [22], a novel framework incorporates DL method into massive multiple-input multiple-output (MIMO) systems to address channel estimation problems. From another viewpoint, the channel matrix is regarded as an image, the better channel estimation performance was obtained by employing a DL based image super-resolution and denoising technique in [23]. Another branch of research attempts to establish a novel endto-end deep neural network (DNN) architecture to replace all modules in communication system, instead of strengthening only certain modules [19], [24]. However, the aforementioned DL based channel estimation methods are implemented by using training data transmitted together with the information data, which increased additional bandwidth consumption. To reduce the overload and fulfill further performance improvement, it is desired to estimate the channel parameters without any pilot data by using the DL method. Different from the above DL based methods, a DNN structure with a pre-trained stacked denoising autoencoder (SDAE) is proposed to estimate the channel

parameters in the chaotic baseband wireless communication system (CBWCS). In contrast to the analytical method using the ACF of chaotic signal in [11], the proposed scheme learns the channel parameters very well, meanwhile, the calculation error and the noise effect are suppressed. The contributions include: 1) A DL based channel estimation method is proposed without any pilot data, in which the pre-trained SDAE is used in the DNN structure to extract the channel state structure information from the ACF of the received signal. 2) The off-line training and online prediction mechanism is designed in the proposed DL based channel estimation scheme, in which the training time is not the application constraint, and the real time computation cost is affordable. 3) Simulation results show the efficiency and superiority of the proposed method in the sense of the smaller mean squared error (MSE) of channel estimation and BER performance, as compared to the other estimation methods.

Existing system

Nowadays confidential data transfer is a crucial task in many multinational companies, military departments, intelligence and surveillance departments, and so on. In such departments and companies lots of efforts are put forth for securing confidential data. Therefore, they need Data encryption and decryption for their applications. An example, which is given below describes data encryption and decryption to secure data using Zigbee wireless communication technology for short and long distances. With help of many encryption and decryption techniques we can achieve the goal of secure communication

Proposed system

Everyone in this world wants to be safe and secure. When it comes to the safety and security of Multinational companies, Military, Army, the situation becomes more complicated. Even a common man puts his maximum efforts to protect his data. One of the popular methods to protect the data in a more secure way is to encrypt the data while sending and when received, decrypt the data to retrieve the original message. Before transmitting the data, the data will be converted into an unreadable form and will be sent. At the receiving end, the reverse of encryption carries on to get back the original message. Thus the data will be protected in every way by following the encryption and decryption standard formats. Wireless makes this project more flexible. Standard algorithms require software to be installed into the system before actually using them and hardwired connections. The hardware connections and cabling can be completely eliminated in this project

Literature survey

S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," Phys. Rev. Lett., vol. 70, no. 20, p. 3031, May 1993.

Control of chaos refers to a process wherein a tiny perturbation is applied to a chaotic system, in order to realize a desirable (chaotic, periodic, or stationary) behavior. We review the major ideas involved in the control of chaos, and present in detail two methods: the Ott–Grebogi–Yorke (OGY) method and the adaptive method. We also discuss a series of relevant issues connected with chaos control, such as the targeting problem, i.e., how to bring a trajectory to a

small neighborhood of a desired location in the chaotic attractor in both low and high dimensions, and point out applications for controlling fractal basin boundaries. In short, we describe procedures for stabilizing desired chaotic orbits embedded in a chaotic attractor and discuss the issues of communicating with chaos by controlling symbolic sequences and of synchronizing chaotic systems. Finally, we give a review of relevant experimental applications of these ideas and techniques. A deterministic system is said to be *chaotic* whenever its evolution sensitively depends on the initial conditions. This property implies that two trajectories emerging from two different closeby initial conditions separate exponentially in the course of time. The necessary requirements for a deterministic system to be chaotic are that the system must be nonlinear, and be at least three dimensional.

A. Dmitriev, A. Kletsov, A. Laktyushkin, A. Panas, and S. Starkov, "Ultrawideband wireless communications based on dynamic chaos," J. Commun. Technol. Electron., vol. 51, no. 10, pp. 1126–1140, Oct. 2006.

In recent years, many communication systems that use a function to encode an information in a chaotic signal were proposed. Since every transmission channel is bandlimited in nature, it is required to determine and to control the chaotic signal spectrum. This way, a bandlimited chaos-based communication system (CBCS) was proposed using digital filters and chaotic synchronization. As the filters modify the original chaotic system, it is necessary to study how their insertion affects chaotic synchronization. In this work, we present a digital discrete-time bandlimited CBCS system analysis, considering practical settings encountered in conventional communication systems. The proposed system is based on master–slave chaotic synchronization and the required conditions for its synchronization is obtained analytically for a general *K*-dimensional chaos generator map. The performance of this system is evaluated in terms of bit error rate. As a way to improve the signal to noise ratio, we also propose to filter the out-of-band noise in the receiver. Numerical simulations show the advantages of using such a scheme. In a digital chaos-based communication system (CBCS), each bit of information is transmitted using a different fragment of a chaotic signal [15], [16]. Thus, it differs fundamentally from the conventional digital communication systems, where each symbol is associated with a constant and predefined waveform.

H. P. Ren, C. Bai, Q. J. Kong, M. S. Baptista, and C. Grebogi, "A chaotic spread spectrum system for underwater acoustic communication," Physica A Stat. Mech. Appl., vol. 478, pp. 77–92, Jul. 2017.

Acoustic communication is a key technology to exchange information underwater, which is of great significance to explore marine resources and to marine defense. The underwater acoustic channel is a time-space-frequency varying channel characterized by serious multipath effect, limited frequency band, complex environmental noises and significant Doppler frequency shift phenomenon, which makes underwater acoustic communication with low Bit Error Rate (BER) to be a

challenging task. A novel chaotic spread spectrum acoustic communication method with low BER is proposed in this paper. A chaotic signal, generated by a hybrid dynamical system, is used as a spread spectrum sequence at the transmitter end. At the receiver end, a corresponding chaotic matched filter is used to offset the effect of multipath propagation and noise. The proposed method does not require the complicated equalization and modulation–demodulation technologies that are necessary for conventional acoustic communication. Simulation results show that the proposed method has good anti-interference ability and lower BER as compared to other traditional methods.

H.-P. Yin and H.-P. Ren, "Direct symbol decoding using GA-SVM in chaotic baseband wireless communication system," J. Frankl. Inst., vol. 358, no. 12, pp. 6348–6367, Aug. 2021.

To retrieve the information from the serious distorted received signal is the key challenge of communication signal processing. The chaotic baseband communication promises theoretically to eliminate the inter-symbol interference (ISI), however, it needs complicated calculation, if it is not impossible. In this paper, a genetic algorithm support vector machine (GA-SVM) based symbol detection method is proposed for chaotic baseband wireless communication system (CBWCS), by this way, treating the problem from a different viewpoint, the symbol decoding process is converted to be a binary classification through GA-SVM model. A trained GA-SVM model is used to decode the symbols directly at the receiver, so as to improve the bit error rate (BER) performance of the CBWCS and simplify the symbol detection process by removing the channel identification and the threshold calculation process as compared to that using the calculated threshold to decode symbol in the traditional methods. The simulation results show that the proposed method has better BER performance in both the static and time-varying wireless channels. The experimental results, based on the wireless open-access research platform, indicate that the BER of the proposed GA-SVM based symbol detection approach is superior to the other counterparts under a practical wireless multipath channel. Filter design and coherent/noncoherent decoding are the key points in communication signal processing [1

H. P. Ren, M. S. Baptista, and C. Grebogi, "Wireless communication with chaos," Phys. Rev. Lett., vol. 110, no. 18, 2013, Art. no. 184101.

The modern world fully relies on wireless communication. Because of intrinsic physical constraints of the wireless physical media (multipath, damping, and filtering), signals carrying information are strongly modified, preventing information from being transmitted with a high bit rate. We show that, though a chaotic signal is strongly modified by the wireless physical media, its Lyapunov exponents remain unaltered, suggesting that the information transmitted is not modified by the channel. For some particular chaotic signals, we have indeed proved that the dynamic description of both the transmitted and the received signals is identical and shown that the capacity of the chaos-based wireless channel is unaffected by the multipath propagation of the physical media. These physical properties of chaotic signals

warrant an effective chaos-based wireless communication system. Nowadays, wireless communication [1,2], ranging from satellite communication and global positioning system (GPS) navigation [3], underwater wireless sensor networks [4], personal mobile phones to portable Wi-Fi applications, is closer to our daily experiences than it used to be. Reliability of the communication is compromised due to several physical constraints affecting the information signal, such as amplitude damping, filtering that causes modification both in the phase and amplitude of the signal, multipath propagation (a signal that travels along many different paths and arrives many times at the receiving location) that causes serious interference, time-varying characteristics, and noise. Wireless communication usually has worse performance than wired channel communication.

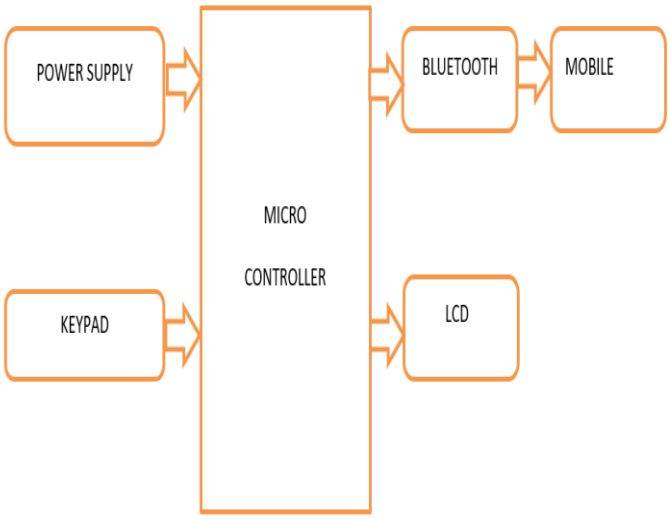
N. J. Corron and J. N. Blakely, "Chaos in optimal communication waveforms," Proc. R. Soc. A Math. Phys. Eng. Sci., vol. 471, no. 2180, Aug. 2015, Art. no. 20150222.

The properties of nonlinear dynamics and chaos are shown to be fundamental to optimal communication signals subject to two practical and realistic design requirements: (i) operation in a noisy environment and (ii) simple hardware implementation. Starting with a simple electronic circuit, a linear filter receiver is presumed, and the matched optimal communication waveform that maximizes the receiver signal-to-noise performance is derived. A return map using samples from this optimal waveform is conjugate to a shift, thereby implying the waveform is chaotic. The optimal communication waveform for a second simple receiver is similarly derived, and it is found to be an exact solution to a physically realizable chaotic oscillator. Thus, a practical consequence of chaos in these waveforms is the potential for simple and efficient signal generation using chaotic oscillators. A conjecture is made that the optimal communication waveform for any stable infinite impulse response filter is similarly chaotic. In modern communications technology, the suitability of a method for conveying information is evaluated in terms of quantifiable metrics, such as performance, efficiency, complexity and cost. A communication method is deemed optimal if it maximizes one or more of these metrics. Pioneering work by Nyquist, Shannon, Wiener and others in the past century established a rigorous theoretical framework for identifying such optimal methods [1,2]. For example, a fundamental performance metric is the signal-to-noise ratio at the receiver. A famous result from communication theory holds that this ratio is maximized by a receiver that forms the correlation of the incoming received waveform with a reference copy of the transmitted waveform [3]. Such a correlation receiver can be practically implemented using a linear filter that has an impulse response that is the time reverse of the transmitted waveform. Such a filter is called a matched filter because it is specifically matched to the transmitted waveform it uses as a reference [4]. For an arbitrary waveform, it may not be practical to realize a matched filter using simple analogue circuits, and more sophisticated digital signal processing is usually required. However, if one presumes a simple analogue matched filter, it is possible to derive the corresponding waveform to

which it is matched. In this paper, we consider two very simple linear filters and derive the corresponding matched waveforms. From this straightforward application of well-established communication theory, we are surprised to learn that the implied optimal communication waveforms are chaotic in the sense of modern dynamical systems theory [5]. Importantly, the presence of chaos enables efficient generation of the waveforms matching these simple filters that otherwise would be impractical. Over the past two decades, many have advocated the development of practical data communications using chaotic waveforms [6–10]. The motivations for such development have been varied. However, in practice, one would choose chaos for communications only if, among all possible choices, a chaotic waveform is optimal in the above sense of maximizing some metric. Here, we consider designing a communication system under two practical and realistic design requirements: (i) operation in a noisy environment and (ii) simple hardware implementation. These requirements do not immediately have any obvious relation to chaotic dynamics. The first requirement suggests the use of a matched filter to obtain a maximal signal-to-noise ratio. The second requirement can be satisfied by selecting a simple, passive analogue filter as the matched filter. To be clear, our design makes no a priori assumption of a role for chaos. However, in two examples, we find that chaos is an implied property of the optimal communication waveforms for these realistic design constraints. In the conclusion, we extrapolate from these results to conjecture that optimal waveforms for a large class of stable matched filters are likewise chaotic. Altogether, these results indicate that the phenomena of nonlinear dynamics and chaos are fundamental and essential to a physical description of optimal communication signals.

IMPLEMENTATION

BLOCK DIAGRAM



CONCLUSION

IoTs represent a class of pervasive systems which exploit embedded sensors (hardware), applications (software which manipulates the hardware), and networks (interconnecting things to transmit data) in smart systems and environments. IoUTs as a specific genre of IoTs rely on underwater sensors which ingest oceanic data in the context of smart oceans. The oceanic data ingested from a multitude of deployed sensors are useful to carry out analysis of multifaceted information relating to marine life, water pollution, or to find water quality parameters. Consequently, it's critical to provide a platform which allows efficient sharing and storage of IoT data in ad-hoc, unsecured environments. To provide a distributed and trustworthy access control mechanism, we have considered

Blockchain technology, specifically Ethereum smart contract to share IoT data. This article offers a system which uses Ethereum blockchain and IPFS for efficient and secure storage of IoT data. It also offers smart contracts to make it easier for users to store and manage access roles for corresponding IoT data. The suggested solution encrypts IoT data sent to IPFS's decentralized storage and records the hash value among different parameters in a blockchain ledger. System evaluation is focused on assessing the performance of data transmission. The solution focuses on decentralizing and securing the data of IoUTs with IoTs system development as a specific genre of the IoTs. This research aims to provide a solution along with a set of guidelines for IoUT practitioners and researchers which can support in the context of the smart ocean to develop the next-generation (software-intensive) of robust and secure blockchain-aided distributed IoT systems. The main purpose of IoUT application is used for decentralizing and sharing the data in an untrustworthy environment. The primary contributions of this research are as follows:

• *Contribution 1* : The access level of data (access management) is implemented to enable data governance, trust-based customizable roles, trustworthiness, and security.

• *Contribution 2* : This research unifies the Internet of Things (IoTs) for effective data sharing, mining, and analyzing oceanic data with Blockchain technology which enables secure management and transmission of relevant data while ensuring performance and efficiency of the proposed solution.

***Future research directions*:** In the future, we will primarily focus on the diversity of data evaluation with more case studies which can further enhance the rigor of evaluation. In addition to the consideration of more case studies and use cases, we also aim to enhance the scalability of the system which can accumulate data from multiple oceanic sites, and centralize the processing and analytics of the data which is being ingested from various distributed sensors.

REFERENCES

[1] Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, 23(5):10–16, 2016.

[2] Statista. Iot and non-iot connections worldwide 2010-2025, 2021.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: a survey. computer networks. *doi*, 10:1016, 2010.

[4] Chien-Chi Kao, Yi-Shan Lin, Geng-De Wu, and Chun-Ju Huang. A comprehensive study on the internet of underwater things: applications, challenges, and channel models. *Sensors*, 17(7):1477, 2017.

[5] Tie Qiu, Zhao Zhao, Tong Zhang, Chen Chen, and CL Philip Chen. Underwater internet of things in smart ocean: System architecture and open issues. *IEEE transactions on industrial informatics*, 16(7):4297– 4307, 2019.

[6] Fraunhofer. Smart ocean technologies solutions for responsible ocean use, 2021.

[7] Eleftherios Kokoris-Kogias, Enis Ceyhun Alp, Sandra Deepthy Siby, Nicolas Gailly, Linus Gasser, Philipp Jovanovic, Ewa Syta, and Bryan Ford. Calypso: Auditable sharing of private data over blockchains. *IACR Cryptol. ePrint Arch., Tech. Rep*, 209:2018, 2018.

[8] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of trust: A decentralized blockchain-based authentication system for iot. *Computers & Security*, 78:126–142, 2018.

[9] Liehuang Zhu, Yulu Wu, Keke Gai, and Kim-Kwang Raymond Choo. Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, 91:527–535, 2019.

[10] Alexander Yakubov, Wazen Shbair, Anders Wallbom, David Sanda, et al. A blockchain-based pki management framework. In *The First IEEE/I- FIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*, 2018.

[11] Shangping Wang, Yinglong Zhang, and Yaling Zhang. A blockchainbased framework for data sharing with fine-grained access control in decentralized storage systems. *Ieee Access*, 6:38437–38450, 2018.

[12] Mingjun Dai, Shengli Zhang, Hui Wang, and Shi Jin. A low storage room requirement framework for distributed ledger in blockchain. *IEEE Access*, 6:22970–22975, 2018.

[13] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *ArXiv preprint arXiv:1407.3561*, 2014.

[14] Gaoqi Liang, Steven R Weller, Fengji Luo, Junhua Zhao, and Zhao Yang Dong. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, 10(3):3162–3173, 2018.

[15] QI Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, 5:14757–14767, 2017.