

GRANT-FREE SAFE-SCMA BASED ON DETECTION OF UNKNOWN ABNORMAL CODEBOOKS

Hanyuan Huang, Tao Li and Hui Zhao

College of Cyber security, Sichuan University, Chengdu, China

ABSTRACT

Non-orthogonal multiple access (NOMA) can support massive accesses in 5G. Sparse code multiple access (SCMA) is a typical NOMA technology. Basic principle of SCMA is that multi-user bit data directly map into multi-dimensional complex sequences through codebooks. Grant-free SCMA allows users to select codebooks from codebook pool to send data instantly, reducing the cost of overhead and delay of granting process. When the receiver and the sender use same codebook information, the data can be transmitted correctly. But in current SCMA researches, the problem of asymmetric codebook information between sender and receiver caused by the intrusion of codebook pool is not considered. In this paper, abnormal codebook detection is proposed in the grant-free SCMA. Because most of intrusion is unknown, initial detection is realised by comparing characteristics of tested codebooks with those legal ones concluded during codebook design process. In this paper, tested objects in the test process can include but not limit to codebook structure, constellations, distribution of constellations, overall feature of codebook pool. Test is executed until discovering error states or accomplishing all tested contents. Inspired by the distinction between self and non self in the artificial immune system, tested abnormal codebooks are saved to act as detectors. To take full advantages of known non-self codebooks, saved detectors are further evolved, and future detection can do match with detectors which are evolved from those known abnormal codebooks to discover some kinds of unknown abnormal codebooks.

KEYWORDS

Grant-free SCMA, SCMA codebooks, abnormal codebooks detection, artificial immune system, abnormal codebook evolution

1. INTRODUCTION

The requirements in 5G include high spectrum efficiency, low latency and massive access. Non-orthogonal multiple access (NOMA) [1-3] allows massive users to share same resources to satisfy these requirements. NOMA is an alternative access technique in 5G. And Sparse Code Multiple Access (SCMA) is a typical example of NOMA. It is able to be demodulated with reasonable complexity by message passing algorithm (MPA) [4]. The principle of SCMA is that multi-user binary data directly maps to multidimensional sparse codewords of SCMA codebooks, where each codeword represents a spread transmission layer, and different layers transmit on the same time-frequency resources. The feature of SCMA multi-user codebooks is one of the keys deciding system performance [5]. The codebooks used for demodulation by the receiver is exactly the same as those used for modulation by the transmitter, which is the necessary prerequisite for correct transmission. In order to save the extra overhead and latency with granting, grant-free SCMA allows users to do data transmission instantly. But the receiver does

not know about which users are currently transmitting data. Because of the instant transmission, all users are less likely to send data at the same time. If each user is assigned a fixed codebook, it will reduce utilization of codebooks. Therefore, in grant-free SCMA, the active users who need to send data select codebooks randomly from the codebook pool for data modulation. The receiver determines the codebook information of active users through corresponding relationship between pilots and codebooks [6].

When problems about security of codebook pool occur, there will be some abnormal codebooks in the codebook pool that the receiver does not contain. If active users select abnormal codebooks for data modulation, receiver will not be able to complete the data demodulation correctly. Therefore, this paper proposes an abnormal codebook detection mechanism. After a user selects a codebook and before modulation, the validity of the codebook is tested firstly. One of the major algorithms to discriminate self and nonself within field of artificial immune systems (AIS) [7] is Negative Selection Algorithm [8]. In NSA, initial detectors are generated randomly and practised by self tolerance to turn into mature detectors. If data matches a detector, it can be seen as abnormal. Because the system is unknown for most abnormal codebooks, the known legal codebook design is prior information in the detection process. A codebook test and detector generation method based on codebook features is proposed, avoiding random detector generation and self tolerance with low efficiency. The test contents can include but not limit to codebook structure, codebook constellations, correlation between constellations. When error states are detected or all contents are completed, the current detection is stopped. If error states are detected, the tested codebook is determined to be abnormal codebook and added to the detector set. To cover the shortage that information of known non-self ones are not taken full advantages of in the conventional NSA, on the premise that a codebook which is very similar to the abnormal codebook can be seen as an abnormal one, the malicious codebook is evolved and stored as detector. The similarity concludes that close Euclidean distance between constellations, or the codebook structure is similar and so on. When the user selects a codebook next time, a tested codebook can match with detectors firstly. If the matching is successful, the codebook will be determined as an abnormal codebook. If the number of detectors does not meet the requirements, codebook test based on codebook features and detector generation are executed continuously.

2. SYSTEM MODELS

2.1. SCMA Modulation

A SCMA [9] encoder can be seen as a mapper from $\log_2 M$ bits to a K -dimensional sparse codeword of a codebook and the size of the codebook is $K \times M$. There are Z ($Z < K$) non-zeros elements in a codeword. Each codeword represents a spread transmission layer. There are J layers, where the j -th layer is expressed as $\mathbf{x}_j = [x_j(1), x_j(2), \dots, x_j(K)]^T$, and $E[\|\mathbf{x}_j(k)\|^2] = 1$. The received signal vector \mathbf{y} over all the subcarriers can be expressed as:

$$\mathbf{y} = \sum_{j=1}^J \text{diag}(\mathbf{h}_j) \mathbf{x}_j + \mathbf{n} \quad (1)$$

Where $\mathbf{h}_j = [h_j(1), h_j(2), \dots, h_j(K)]^T$ is the channel gain for the j -th layer. And $\text{diag}(\cdot)$ refers to a diagonal matrix, in which the k -th element on the diagonal is $h_j(k)$. The process of SCMA is shown in Figure.1 with $M=4$, $K=4$ and $Z=2$.

The received signal in the k -th subcarrier resource is:

$$y(k) = \sum_{j \in \varphi_k} h_j(k) x_j(k) + n(k) \quad (2)$$

Where $h_j(k)$ is the channel gain for the j -th layer in the k -th resource and $n(k)$ is complex Gaussian noise in the k -th resource. φ_k is a set made up with all the layers in the k -th resource and its cardinality is d_f , which means d_f layers occupying the k -th resource.

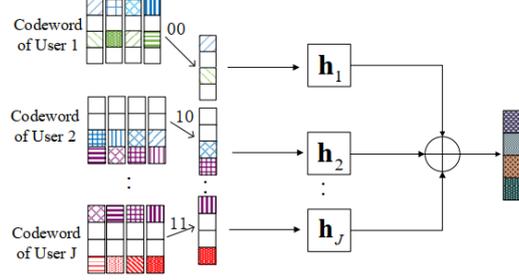


Figure 1. The process of SCMA ($J = 6, K = 4, Z = 2$).

2.2. SCMA Demodulation

Message Passing Algorithm (MPA) is usually used to do SCMA decoding. MPA is an iterative detection algorithm with optimal BER (Bit Error Rate) performance and acceptable computational complexity. MPA estimates the transmitted vector $\tilde{\mathbf{x}}_j$ through the received signal \mathbf{y} . The initialization of confidential information in the k -th resource of MPA can be written as:

$$\Phi_k = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{1}{2\sigma^2} \left\| y(k) - \sum_{j \in \varphi_k} h_j(k) x_j(k) \right\|^2\right) \quad (3)$$

Where σ refers to the noise variance. Each MPA iteration consists of two steps: i) passing confidential information from resource nodes to user nodes; ii) information exchange from user nodes to resource nodes. Then, a posteriori probability for the corresponding codeword \mathbf{x}_j . The binary log-likelihood ratios (LLRs) is used to decide what the $\log_2 M$ bits are.

The basic condition for correct SCMA transmission is keeping equal codebook information between transmitter and receiver.

2.3. Grant-free SCMA

In grant-free transmission, terminals will not wait for a transmission grant from the base station, which saves a lot of overhead and latency with granting. We defined users doing the transmission as active users, and others having no transmission as inactive users. When an active user needs to send message, it randomly selects a codebook from the codebook pool to modulate bit data. There are N codebooks totally. Active users select codebooks randomly from N codebooks to modulate data. The receiver can do active user detection and confirm codebooks being selected through active pilots detection based FOCUSS or EM algorithm [10]. It is possible that different active users select same codebook. But the receiver still can demodulate data with inferior but not nonlethal performance, as long as information of codebook pool saved by receiver is same as that in transmitter.

3. SCMA CODEBOOKS

The SCMA codebook structure can be represented by factor graph or mapping matrix. The edge between layer node and resource node in factor graph or the non-zero element in k -th row and j -th column of mapping matrix means that the k -th resource is occupied by the j -th layer. Mapping matrix of a simple codebook example, where $M=4, J=6, K=4, d_f=3, Z=2$ in [11] is shown as:

$$F_{4 \times 6} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \quad (4)$$

A layer is equipped with a complex constellations set S_u ($u = 0, 1, \dots, d_f - 1$) in one-dimensional resource. The cardinality of S_u is M . All elements in S_0 are reals and other $S_u = e^{j\theta_u}S_0$. The factor graph of the codebook example in [11] is shown in Figure.2 and $y(k)$, $h_j(k)$, $x_j(k)$ express same meanings as Eq. (2). The overload rate is $\lambda = J/K = 150\%$. Besides, $x_1(1) \in S_0$, $x_3(1) \in S_1$, $x_5(1) \in S_2$. And constellations points in Fig.2 express that $S_1 = e^{j\theta_1}S_0$ and $S_2 = e^{j\theta_2}S_0$, $\theta_1 < \theta_2 \dots < \theta_{d_f-1}$. Besides, the combination $\{S_0, \dots, S_{d_f-1}\}$ is reused in every resource, which means an example of constellations allocation in all resources based on Eq.(4) can be expresses as:

$$F_{4 \times 6} = \begin{bmatrix} S_0 & 0 & S_1 & 0 & S_2 & 0 \\ 0 & S_2 & S_0 & 0 & 0 & S_1 \\ S_1 & 0 & 0 & S_0 & 0 & S_2 \\ 0 & S_0 & 0 & S_2 & S_1 & 0 \end{bmatrix} \quad (5)$$

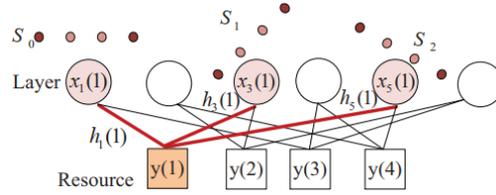


Figure 2. Factor graph of a SCMA codebook ($J = 6$, $K = 4$, $d_f = 3$, $Z = 2$).

In the iterative process of MPA demodulation, after calculating the confidential information of all codeword symbols on each resource separately, the confidential information is transferred between different resources and users. So, when considering the problems about constellation points, such as extraction of codebook feature and codebook design, it is feasible to be focus on those of one-dimensional resource. And when considering problems about codebook structure or constellations allocation in entire codebook, it is still necessary to think about all resources.

4. SAFE-SCMA DETECTING UNKNOWN ABNORMAL CODEBOOKS

In the condition that most of intrusion is unknown, useful prior information is normal features in the codebook design. After a user selects a codebook from codebook pool, the codebook should be estimated its validity. Obviously if normal codebooks are much more than abnormal codebooks, the probability that an abnormal one is selected is fairly low. It can satisfy high-reliability requirements in 5G. So, it is necessary to have a detection with large number of normal codebooks and acceptable complexity of computation. AIS has nature advantages in unknown intrusion detection because of self renewal and evolution. But discrimination between self and nonself in the typical algorithm NSA spends high computation complexity in random initial detector generation and tolerance with self set. It will have a strong impact on low-latency business in 5G. In the initial codebook test without detectors we propose a method based on codebook feature extraction. And tested abnormal codebooks are saved and evolved to act as detectors, which overcomes the shortcomings with aimlessness of detector generation and insufficient use of known abnormal data in the traditional NSA.

4.1. Initial Codebook Test and Detector Generation

Initial codebook test and detector generation based on codebook features are proposed, avoiding random generation and matching with all self codebooks. The test contents are based on the extraction of normal codebook features. The test process is carried out until the abnormal state is detected or all test steps are completed. A codebook with abnormal states can act as a detector. The following contents are about some codebook features for test.

4.1.1. Codebook Structure

There is a $K' \times M'$ tested codebook. It is set of K' -dimensional sparse codewords. There are Z' ($Z' < K'$) non-zeros elements in a codeword. And a normal codebook should be a $K \times M$ one with Z non-zeros elements in a codeword. We can compare K' and K , M' and M , Z' and Z . If results are not all equivalence, the tested codebook is judged as an abnormal one. When comparison results are coincident, positions of non-zero elements in each codewords should be same and conform to one column of the mapping matrix (Eq. (4) is an example) in the codebook pool.

4.1.2. Values of Constellations

There is a $K' \times M'$ tested codebook. It is a set of K' -dimensional sparse codewords. Extract non-zero elements from one resource and note as $\{C_1, \dots, C_{M'}\}$. Firstly, detect whether these elements are on a straight line in the complex rectangular coordinate system. If so, then see whether the angle corresponding to this line belongs to $\{\theta_1, \dots, \theta_{d_f-1}\}$ decided in the codebook design. If the tested codebook cannot meet these conditions, it is an abnormal one.

4.1.3. Power of Codewords

The m -th codeword in the tested codebook is noted as $\mathbf{x}_m = [x_m(1), x_m(2), \dots, x_m(K)]^T$. To keep the fair of power allocation, different codewords should have the same average power, which means $E[\|\mathbf{x}_m(k)\|^2] = 1$.

4.1.4. Distribution of constellations

Non-zero elements on one resource form a straight line in the complex rectangular coordinate system. It can be found that Z' lines can be extracted in a tested codebook. And there are Z' angles $\{\theta'_1, \dots, \theta'_{Z'}\}$. We can determine constellation distribution of the tested codebook should belong to which column in Eq. (5). Because it is decided that $S_u = e^{j\theta_u} S_0$, $\theta_1 < \theta_2 \dots < \theta_{d_f-1}$, and differences between θ_u in codebook design, we can judge whether the distribution of constellations meets the criterion in Eq. (5) through the difference between angles.

4.2. Detector Evolution

In conventional AIS, when a new detector generates, the process of random generation and tolerance with large self set are repeated. Previous detection information is not used for detector generation. It causes poor efficiency and waste of previous work. If an abnormal codebook that has been detected is evolved, the evolved results can be seen as a detector that can highly match with abnormal codebooks on a high probability.

All of detected abnormal codebooks and evolved ones are saved as detectors. The criterion of evolution can include but not limit to close Euclidean distance between constellations, the similar codebook structure, or exchange of constellation position. When the next codebook selection occurs, tested codebook is taken to match with detectors firstly. If the matching is successful, the codebook will be determined as an abnormal codebook. When matching fails, a detection based on legal codebook features is carried out. If the number of detectors evolved from one known codebook is meet the requirements, it is considered that a kind of unknown abnormal codebooks can be detected only by detectors. But it is still needed to regularly update detectors.

5. CONCLUSIONS

When there is a malicious codebook unknown to the receiver in the codebook pool of grant-free SCMA, it will seriously affect correct demodulation of data. Most malicious codebooks are unknown, and AIS can do unknown data detection because of its adaptability and evolutionary ability. In this paper, we do initial abnormal codebook test based on legal codebook features, that are concluded during the process of codebook design. If a codebook has abnormal features, it is an abnormal one. And tested abnormal codebooks can be used to generate detectors. That avoids low efficiency caused by random generation and direct tolerance with large self set in the typical algorithm NSA. To take advantages of existing detectors, part of new detectors can be generated through evolution of existing detectors. That improves deficiencies about waste of previous detector' information. In the subsequent detection, codebooks to be tested can be matched with detectors or tested by using normal codebook features. When existing detectors can cover most kinds of abnormal states, we can consider that we will get a responsible result only by detectors. To keep adaptability of detectors, regularly update of detector set is necessary.

ACKNOWLEDGEMENTS

This work was partially supported by Natural Science Foundation of China (Grant No.U1736212, No.61572334, No.61872255), Sichuan Province Key Research and Development Project of China (Grant No.2018GZ0183), Sichuan University (Grant No. YJ201933); the China Postdoctoral Science Foundation (Grant No. 2019TQ0217) the Fundamental Research Funds for the central Universities, the National Key Research and Development Program of China (Grant No.2016YFB0800600).

REFERENCES

- [1] Saito Y, Kishiyama Y, Benjebbour A, et al. Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access[J]. 2013, 14(6):1-5.
- [2] Moshavi S. Multi-user detection for DS-CDMA communications[J]. IEEE Communications Magazine, 1996, 34(10):124-136.
- [3] Ping L, Liu L, Wu K, et al. Interleave division multiple-access[J]. IEEE Transactions on Wireless Communications, 2006, 5(4):938-947.
- [4] Huawei. Innovate Asia: First 5G algorithm competition [EB]. 2015.
- [5] Alam, Mehmood, and Q. Zhang. "Performance Study of SCMA Codebook Design." Wireless Communications and Networking Conference IEEE, 2017.
- [6] Au, Kelvin, et al. "Uplink contention based SCMA for 5G radio access." GLOBECOM Workshops IEEE, 2015:900-905.

- [7] Forrest S, Beauchemin C. Computer immunology[J]. Immunological Reviews, 2007, 216(1):176-197.
- [8] S. Forrest, A. S. Perelson, Allen L, et al. Self-nonsel self discrimination in a computer[C]. In: Proceedings of the 1994 IEEE Symposium on Security and Privacy, IEEE Computer Society, 1994.
- [9] Huawei. Innovate Asia: First 5G algorithm competition [EB]. 2015.
- [10] Bayesteh, Alireza, et al. “Blind detection of SCMA for uplink grant-free multiple-access.” International Symposium on Wireless Communications Systems IEEE, 2014:853-857.
- [11] Hanyuan Huang, Hui Zhao, Feilong Wang, and Jing Li, Uplink Grant-free Multi-codebook SCMA Based on High-overload Codebook Grouping, IEEE /CIC International Conference on Communications in China Workshops, 2018.

AUTHORS

Hanyuan Huang received the M.S. degree in information and Communication Engineering from Beijing University of Post and Telecommunication, Beijing, China, in 2019. She is currently pursuing the Ph.D. degree with the College of Computer Science in Sichuan University, Chengdu, China. His research interests include network security, artificial immune systems, intrusion detection, and communication engineering.



Li Tao received the Ph.D. degree in computer science from the University of Electronic Science and Technology of China, in 1994. He is currently a Professor with the College of Cyber Security, Sichuan University, China. His main research interests include network security, artificial immune systems, cloud computing, and cloud storage.



Hui Zhao received the Ph.D. degree in computer science from the Sichuan University, Chengdu, China, in 2011. He is currently an associate professor with the College of Cyber Security, Sichuan University, China. His main research interests include network security, information security, embedded system.

