Joint Virtual User Identification and Channel Security En/Decoding Method for Ad hoc Network

Kenan Zhang†, Xingqian Li†, Kai Ding† and Li Li††

† Beijing Institute of Spacecraft System Engineering, Beijing, 100094 China
†† Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100083 China

Summary
Ad hoc network is self-organized network powered by battery. The reliability of virtual user identification and channel security are reduced when SNR is low due to limited user energy. In order to solve this problem, a joint virtual user identification and channel security en/decoding method is proposed in this paper. Transmitter-receiver-based virtual user identification code is generated by executing XOR operation between orthogonal address code of transmitter and pseudo random address code of receiver and encrypted by channel security code to acquire orthogonal random security sequence so as to improve channel security. In order to spread spectrum as well as improve transmission efficiency, data packet is divided into 6-bit symbols, each symbol is mapped with an orthogonal random security sequence. Subspace-based method is adopted by receiver to process received signal firstly, and then a judgment model is established to identify virtual users according to the previous processing results. Simulation results indicate that the proposed method obtains 1.6dB E_b/N_0 gains compared with reference methods when miss alarm rate reaches 10^{-3}.

Keywords:
Ad hoc network, Joint en/decoding method, Virtual user identification, channel security

1. Introduction

Ad hoc network is self-organized network powered by battery. Limited user energy raises the issue of reliability of virtual user identification and channel security. In order to solve this problem many virtual user identification methods have been proposed by researchers in recent years. In literature [1], transmitter-based code is used to spread data packet, and receivers identify active users firstly and then extract address information of destination user from packet header to judge virtual users. This method consumes more energy and the channel security is weak, therefore a transmitter-receiver based spreading code is constructed in literature [2]. By using this code to spread data packet, receivers don't need to extract address information of destination user from packet header and thus reduce the energy consumption. However, the performance of this method degrades when the network is overloaded. Therefore, spreading codes for overloaded networks is designed in literature [3], and virtual users can be identified by using the maximum likelihood decoding method. The above methods are designed from the perspective of spreading code construction. Literature [4] proposes a method based on random set theory, which has good performance but high complexity. To address this problem, literature [5] uses tree search technique to reduce complexity. Different from the random set theory-based method, literature [6] proposes a per-survivor processing method similar to Viterbi algorithm and two particle filtering based methods to identify virtual users which are all based on traditional probabilistic theory. Unlike the above probabilistic methods, literature [7] proposes a deterministic method based on algebraic theory to identify virtual users within a certain delay by designing a protocol sequence with good inter-correlation properties that allow users to identify virtual users based on channel activity information only. In [8], a cross-layer approach is proposed from the perspective of protocol design to use the pseudo-random scheduling table in MAC layer protocol SEEDEX [9] to identify virtual users. Literature [10-12] address the problem of virtual user identification in massive Machine Type of Communication (mMTC). Literature [10] proposes a compressed sensing-based method to identify virtual users. Literature [11] introduces an expectation propagation algorithm based on compressed sensing to reduce miss alarm rate and false alarm rate of virtual user identification. Literature [12] proposes a deep neural network-based method for virtual user identification, which effectively reduces miss alarm rate and false alarm rate of virtual user identification.

All the methods introduced above suffer from high miss alarm rate and false alarm rate especially under low SNR and do not consider channel security. In this paper, a joint virtual user identification and channel security en/decoding method is proposed for ad hoc network. Transmitter-receiver based virtual user identification code is generated and encrypted by channel security code to obtain orthogonal random security sequence in order to enhance channel security. Data packet are divided into 6-bit symbols, and each symbol is corresponded to an orthogonal random security sequence so as to spread spectrum and improve transmission efficiency. A subspace-based method is adopted by receiver to process received signal firstly, and then a judgment model is established to identify virtual users according to the

Manuscript received November 5, 2022
Manuscript revised November 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.11.35

previous processing results. Simulation results show that the proposed method reduces miss alarm rate and false alarm rate of virtual user identification.

2. Joint virtual user identification and channel security encoding method

2.1 Transmitter address code and receiver address code

In ad hoc network users communicate directly with each other without a central node. In order to identify virtual users, two codes w and p are assigned to each user. w is called transmitter address code and p is called receiver address code. Assuming that there are no more than 64 users in ad hoc network, 64-bits Walsh code is used as transmitter address code and 64-bits M sequence is used as receiver address code. Walsh codes and M sequence are shown in Table 1 and Table 2 respectively. Both Table 1 and Table 2 are stored in each user.

Table 1. Walsh codes

Number	Walsh codes
1	01101001100101101001011001101001 10010110011010010110100110010110
……	……
64	01100110011001100110011001100110 01100110011001100110011001100110

Table 2. M sequences

Number	M sequences
1	11011111101011100011001110110000 00111100100101010011010000100010
……	……
64	01011011111101011100011001110110 00000111100100101010011010000100

Each user is numbered and the number of user is used as the index of Table 1 and Table 2. Suppose user 1 intends to transmit to user 2, user 1 searches Table 1 with its number to get transmitter address code w_1, and searches Table 2 with the number of user 2 to get receiver address code p_2. And then user 1 generates virtual user identification code v_{12} by executing XOR operation shown in Eq. (1). Data packets don't need to contain the address information of destination user in its header since v_{12} contains user 2's receiver address code. In this way the security of user 2's receiver address code is enhanced at the same time the energy consumption of user 2 is reduced by avoiding extracting the address information of destination user from packet header.

$$v_{12} = w_1 \oplus p_2 \tag{1}$$

Since Walsh codes are orthogonal as shown in Eq. (2), in which N_w denotes code length, symbol "+1" denotes bit "0" and symbol "-1" denotes bit "1". Therefore, using Walsh codes as transmitter address codes can make the signals coming from different transmitters at the same symbol interval orthogonal to each other, which enhances the ability to resisting multiple access interference of v_{12}.

$$\frac{1}{N_w}\sum_{l=1}^{N_w} w_a(l)\, w_b(l) = \begin{cases} 1, & a = b \\ 0, & a \neq b \end{cases} \tag{2}$$

Since M sequences have a strong autocorrelation shown in Eq. (3), in which N_p denotes code length, symbol "+1" denotes bit "0" and symbol "-1" denotes bit "1". Therefore, using M sequence as receiver address code enhances the ability to resisting inter-symbol interference of v_{12}.

$$\frac{1}{N_p}\sum_{l=1}^{N_p} p_a(l)\, p_a(l+m) = \begin{cases} 1, & m = 0 \\ 0, & m \neq 0 \end{cases} \tag{3}$$

2.2 Spectrum spreading and data transmission

A list of channel security codes shown in Table 3 is also stored in each user which consists of 64 true random sequences [13]. XOR operation is executed between v_{12} and channel security codes z_c, c=1,..,64 in Table 3 as shown in Eq. (4) to obtain 64-bit orthogonal random security sequences $s_{1,2,c}$,c=1,..,64.

Table 3. Channel security codes

Number	Channel security codes
1	10011101110001111111100010101100 10101011101000110101000100101000
……	……
64	01011000100101010110011101111001 01001001011001010010001010001001

Data packet transmitted by user 1 is divided into 6-bit groups, and each group is considered as a symbol. Therefore, there are 64 kinds of symbols, and each symbol is mapped with an orthogonal random security sequence to achieve spectrum spreading as shown in Table 4. With this spectrum spreading method, bandwidth can be saved and transmission efficiency can be improved.

Table 4. Orthogonal random security sequences

6-bit symbol	Orthogonal random security sequences
000000	01001011000011010000100110100101 01000100111000000101000011111011
……	……
111111	10001110010111111001011001110000 10100110001001100010001101011010

$$s_{1,2,c} = v_{12} \oplus z_c,\ c = 1,2,\cdots,64 \tag{4}$$

In order to coordinate the behavior of each user in ad hoc network we assume each user is either in "Listen" state ("L" for short) or "Possibly Transmit" state ("PT" for short) in each symbol interval. When user is in "L" state, it can only receive signal; when user is in "PT" state, it can only transmit signal with a certain probability. "PT" state is indicated by binary symbol "1", and "L" state is indicated by binary symbol "0". The state of each user is controlled by a scheduling table which is generated by pseudo random sequence generator. Each user generates its scheduling table with a same pseudo random sequence generation polynomial and with its number as the initial state. Each user periodically inverts the rightmost bit of the initial state and cyclically shifts one bit right to generate new initial state in order to update the scheduling table. User 1 generates the scheduling tables of all users and finds a symbol interval in which user 1 is in "PT" state while user 2 is in "L" state, and if there are α users in the network that are also in "PT" state, then user 1 transmits with probability min{γ/(α+1),1} in which γ is a parameter that can be adjusted. The use of scheduling table to coordinate the behavior of each user can avoid network congestion and at the same time reduce the amount of computation of user 2.

3. Joint virtual user identification and channel security decoding method

Consider an ad hoc network with Q users who transmit synchronously over an additive white Gaussian noise (AWGN) channel. Assuming that there are H active users transmitting at the current symbol interval. Since there is no central node in ad hoc network, user 2 that in "L" state can receive all packets transmitted in the current symbol interval, and the purpose of virtual user identification for user 2 is to identify the packets transmitted to itself from the received packets. The received signal $r(t)$ can be expressed as

$$r(t) = x(t) + n(t), t \in [0, T] \tag{5}$$

where T denotes symbol interval, $n(t)$ is the AWGN signal. $x(t)$ is the superposition of the signals transmitted by H active users, which can be expressed as

$$x(t) = \sum_{h=1}^{H} y_h(t), t \in [0, T] \tag{6}$$

$y_h(t)$ indicates the signal transmitted by the hth active user, which has the following form

$$y_h(t) = \sum_{l=0}^{N-1} \beta_l^h g(t - lT_c), t \in [0, T] \tag{7}$$

where $\beta_0^h\beta_1^h\ldots\beta_{N-1}^h$ is the orthogonal random security sequence transmitted by the hth active user. N denotes the length of $\beta_0^h\beta_1^h\ldots\beta_{N-1}^h$, whose value is 64. Orthogonal random security sequence comprises "+1" which denotes bit "0" and "-1" which denotes bit "1". $g(t)$ is normalized rectangular pulse of duration T_c. T_c and T has the relationship of $T_c/T=N$.

Substituting Eq. (6) into Eq. (5) yields

$$r(t) = \sum_{h=1}^{H} y_h(t) + n(t), t \in [0, T] \tag{8}$$

Chip-matched filtering followed by sampling transforms $r(t)$ into vector form $\boldsymbol{r} \in \mathrm{R}^N$ which is shown in Eq. (9).

$$\boldsymbol{r} = \sum_{h=1}^{H} \boldsymbol{y}_h + \boldsymbol{n} \tag{9}$$

where $\boldsymbol{y}_h=[\beta_0^h\beta_1^h\ldots\beta_{N-1}^h] \in \{\pm 1\}^N$ denotes the vector transmitted by the hth active user, $n \in \mathrm{R}^N$ is assumed to be AWGN vector with zero-mean and covariance matrix $\sigma^2\mathbf{I}_N$.

The auto-covariance matrix of $\boldsymbol{r}$ can be written in this form

$$\boldsymbol{CovR} = \mathrm{E}\{\boldsymbol{r}\boldsymbol{r}^{\mathrm{T}}\} \tag{10}$$

Since the orthogonal random security sequences transmitted by different active users are orthogonal to each other, we have

$$\boldsymbol{CovR} = SS^{\mathrm{T}} + \sigma^2\mathrm{I}_N \tag{11}$$

where $\boldsymbol{S}=[\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_H] \in \mathrm{R}^{N\times H}$. Let set $A=\{\boldsymbol{y}_1,\boldsymbol{y}_2,\ldots,\boldsymbol{y}_H\}$. Eigenvalue decomposition (EVD for short) of $\boldsymbol{CovR}$ is performed as

$$\boldsymbol{CovR} = U\Lambda U^{-1} \tag{12}$$

$\boldsymbol{U}$ is orthogonal matrix due to $\boldsymbol{CovR}$ is symmetric, we obtain

$$\begin{aligned}\boldsymbol{CovR} &= U\Lambda U^{\mathrm{T}} \\ &= [U_{\mathrm{s}} \quad U_{\mathrm{n}}]\begin{bmatrix}\Lambda_{\mathrm{s}} & 0 \\ 0 & \Lambda_{\mathrm{n}}\end{bmatrix}\begin{bmatrix}U_{\mathrm{s}}^{\mathrm{T}} \\ U_{\mathrm{n}}^{\mathrm{T}}\end{bmatrix}\end{aligned} \tag{13}$$

Combining Eq.(11) with Eq.(13) yields

$$SI_H S^{\mathrm{T}} = U_{\mathrm{s}}(\Lambda_{\mathrm{s}} - \sigma^2 I_H)U_{\mathrm{s}}^{\mathrm{T}} \tag{14}$$

where range($\boldsymbol{U}_{\mathrm{s}}$) is called signal subspace. It can be seen that range($\boldsymbol{S}$)=range($\boldsymbol{U}_{\mathrm{s}}$).

User 2 generates the scheduling tables of all users, and searches all the scheduling tables in current symbol interval to find the set of users in "PT" state denoted by E. And then user 2 generates the set of virtual user identification codes denoted by V_2 via executing XOR operation between p_2 and the transmitter address code of each user in E. Finally, user 2 generates the set of orthogonal random security sequences denoted by B_2 by executing XOR operation between each element of V_2 and the channel security codes in Table 3.

The orthogonal random security sequences transmitted by virtual users of user 2 is represented by set A_2. Since $A_2=A\cap B_2$, the purpose of virtual user identification is to identify the sequences belonging to A from B_2. If A_2 is not empty, the orthogonal random security sequences in A_2 belong to range($\boldsymbol{S}$) and also belong to range($\boldsymbol{U}_{\mathrm{s}}$). Therefore projecting the orthogonal random security sequences in B_2 into $\boldsymbol{U}_{\mathrm{s}}$ as shown in Eq.(15) yields confidences set $D_2=\{d_{i,2,c}, i \in E, c=1,2,\ldots,64\}$.

$$d_{i,2,c} = \left\|U_{\mathrm{s}}^{\mathrm{T}} s_{i,2,c}\right\|^2 = (U_{\mathrm{s}}^{\mathrm{T}} s_{i,2,c})^{\mathrm{T}}(U_{\mathrm{s}}^{\mathrm{T}} s_{i,2,c}), s_{i,2,c} \in B_2 \tag{15}$$

Assuming that subspace estimation error can be ignored. If user i in E is the virtual user of user 2, then there must exist $s_{i,2,c}$ in B_2 generated by user i that belongs to both B_2 and A, then its corresponding $d_{i,2,c}$ satisfies $d_{i,2,c}=N$. Conversely, if user i in E is not the virtual user of user 2, then the orthogonal random security sequences generated by user i belong to B_2 but not A, then the confidences of user i in D_2 obey $0 \le d_{i,2,c} < N, c = 1,2,\cdots,64$. In this ideal case, user 2 can easily identify virtual users based on the result of Eq.(15). However, in the real case, due to the effect of unavoidable subspace estimation error and channel noise, the confidences of user i also obey $0 \le d_{i,2,c} < N, c = 1,2,\cdots,64$, even if user i is a virtual user of user 2.

Therefore, in this paper a judgment model shown in Eq.(16) is established to distinguish virtual users from non-virtual users, in which d_{th} denotes judgment threshold which is an experimental value. User 2 identifies its virtual users by comparing the confidences in D_2 with d_{th}.

$$A_2 = \{s_{i,2,c} \mid d_{i,2,c} \ge d_{th}, s_{i,2,c} \in B_2, d_{i,2,c} \in D_2\} \quad (16)$$

If all the confidences in D_2 are less than d_{th}, it means that user 2 doesn't have virtual user. Then user 2 discards the received signal without subsequent processing; if there exist $d_{i,2,c}$ meets $d_{i,2,c} \ge d_{th}$, it means that user i is the virtual user of user 2; if there exist more than one confidence of user i that are no less than d_{th}, then choose the orthogonal random security sequence corresponding to the largest confidence as index to search Table 4 so as to find the 6-bit symbol transmitted by user i.

4. Numerical results

The simulation scenario is shown in Fig. 1. All the users keep static and transmit in AWGN channel synchronously with BPSK modulation format. One user is randomly selected as the observation user, and it keeps in "L" state all the time during the simulation, while the states of the other users at each symbol interval are determined by their scheduling tables. The user in "PT" state transmits data packet with equal probability, and chooses one user in "L" state as its destination user randomly. The experimental results is obtained over 1000 independent simulations. The parameters of the simulation is shown in Table 5, in which PL represents packet length,.

Table 5 Simulation parameters

Simulation parameters	Value
PL	1200bits
N	64bits
T	2×10^{-6}s

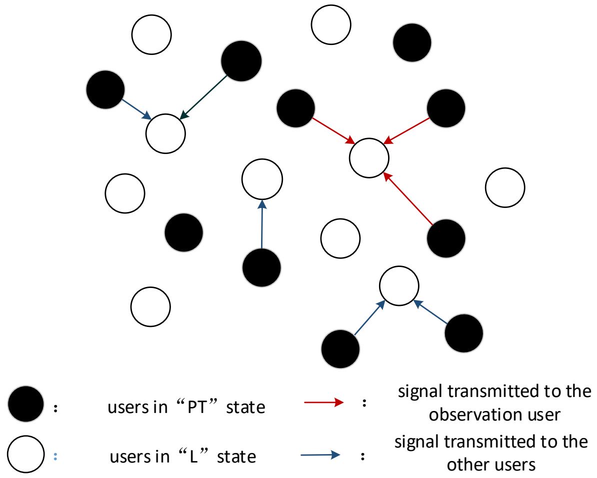


Fig. 1 Structure of ad hoc network

4.1 The choice of d_{th}

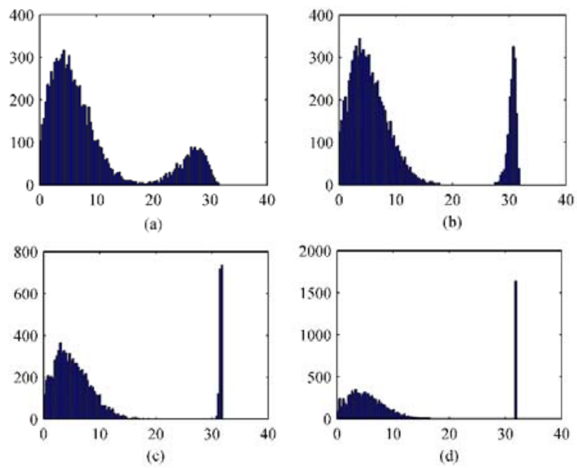
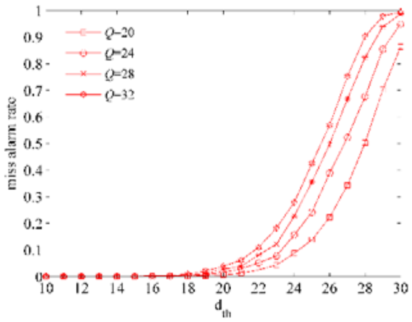
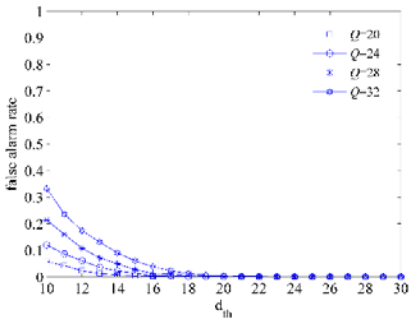


Fig.2 Confidence histogram

Fig. 2 shows the distribution of confidence of virtual users and non-virtual users when E_b/N_0 takes -5dB,-3dB,-1dB,4dB corresponding to Fig.2(a),(b),(c),(d) respectively conditioning that Q =20. With the increase of E_b/N_0, the difference between the confidence of virtual users and non-virtual users becomes more and more obvious. Therefore it is only necessary to choose d_{th} under the worst case of E_b/N_0. The d_{th} suitable for E_b/N_0=-5dB is also suitable for E_b/N_0=-4.5dB~4dB therefore the choice of d_{th} has good adaptability to wireless environment.



(a) Miss alarm rate VS d_{th}



(b) False alarm rate VS d_{th}

Fig. 3 The relationship between miss alarm rate and false alarm rate of the proposed method and d_{th} when E_b/N_0=-5dB,Q=20,24,28,32

Fig. 3 shows the curves of miss alarm rate and false alarm rate of the proposed method versus d_{th} when Q takes 20, 24, 28, and 32 respectively conditioning that E_b/N_0=-5dB. Miss alarm rate indicates the probability that a user is virtual user but is judged as non-virtual user, while false alarm rate indicates the probability that a user is non-virtual user but is judged as virtual user. We can see that miss alarm rate ascends and false alarm rate descends as d_{th} increases. The trend of the curve is basically same for different Q, therefore the choice of d_{th} has good adaptability to user number.

In order to make a balance between miss alarm rate and false alarm rate, d_{th} is set to be 22.

4.2 Comparison of miss alarm rate and false alarm rate

We compare miss alarm rate and false alarm rate between the proposed method and four reference methods advocated in literature [6] and [7]. Three reference methods advocated in literature [6] are called Sequential Importance Sampling-optimal (SIS-OPT for short), Sequential Importance Sampling-linear filter (SIS-LF for short), and Per-Survivor Processing (PSP for short). One reference method advocated in literature [7] is called User Detectable Sequence (UDS for short).

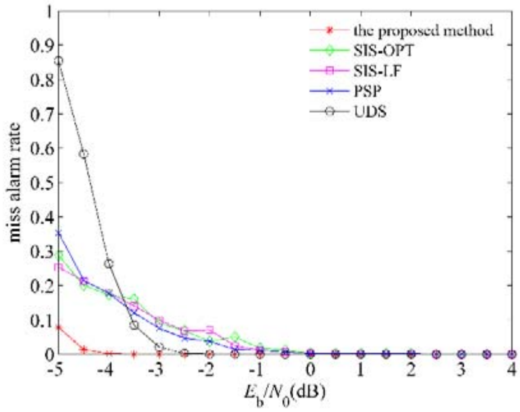


Fig. 4 Miss alarm rate VS E_b/N_0 under Q=20

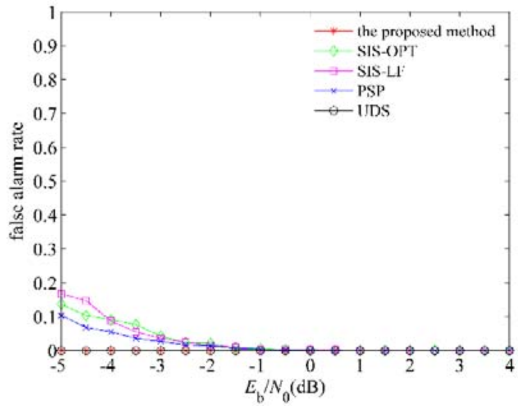


Fig. 5 False alarm rate versus E_b/N_0 under Q=20

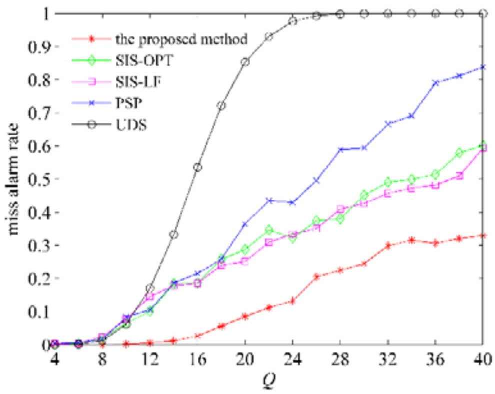


Fig. 6 Miss alarm rate versus Q under E_b/N_0=-5dB

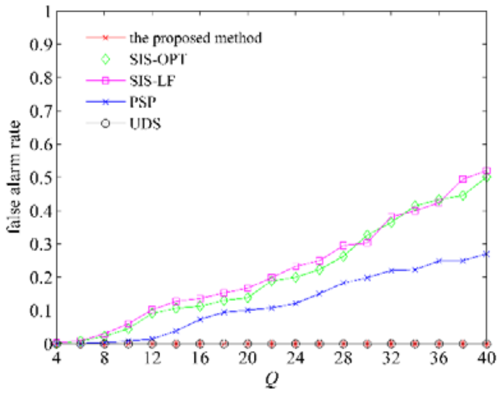


Fig. 7 False alarm rate versus Q under E_b/N_0=-5dB

Fig. 4 and Fig. 5 compare miss alarm rate and false alarm rate of the proposed method with that of the reference methods under different E_b/N_0 conditioning that Q=20 respectively. It can be seen from Fig.4 that the performance of UDS is poor under low E_b/N_0 due to the fact that the method is designed under ideal conditions. The proposed method achieves at least 1.6dB E_b/N_0 gains when miss alarm rate reaches 10^{-3} comparing with the other four methods. It can be seen from Fig. 5 that the curve of false alarm rate of the proposed method coincides with that of UDS, which is zero under all E_b/N_0.

Fig. 6 and Fig. 7 compare miss alarm rate and false alarm rate of the proposed method with that of the reference methods under different Q conditioning that E_b/N_0=-5dB respectively. It can be seen from Fig. 6 that the performance of UDS is close to that of the proposed method when $Q \leq 8$ and the gap between them gradually enlarges with the increase of Q. In Fig. 7, the curve of false alarm rate of the proposed method coincides with that of UDS once again being zero under all Q, which is consistent with the performance shown in Fig. 5.

It can be seen from Fig. 4 to Fig. 7 that the performance of the proposed method is the best among all the five methods, especially under the case of low E_b/N_0 and large number of users. This is due to the characteristics of orthogonal random security sequence, which makes the proposed method resist multi-access interference and inter-symbol interference effectively.

4.3 Analysis of complexity

The complexity of the proposed method is analyzed in this chapter. To simplify the analysis, it is assumed that the complexity of basic operations such as multiplication, addition and comparison is set to be unit one. The number of users that in "PT" state is denoted by PH and the number of virtual users of user 2 is denoted by F. The total complexity is obtained by calculating the complexity of each step of the proposed method.

The complexity of the proposed encoding method:

Step 1: User 1 generates virtual user identification code with complexity of N;

Step 2: User 1 generates orthogonal random security sequences with complexity of $64\times N$.

The complexity of the proposed decoding method:

Step1: User 2 computes ***CovR*** with complexity of $2N^2\times H-N^2+N$;

Step2: User 2 executes EVD of ***CovR*** with complexity of N^3.

Step3: User 2 generates B_2 with complexity of $65\times N\times PH$;

Step4: User 2 generates D_2 with complexity of $64\times PH\times(2N\times H+H-1)$;

Step5: User 2 compares confidences in D_2 with d_{th} with complexity of $64\times PH$;

Step6: User 2 get 6-bit symbols with complexity of $65\times N\times F$. Let F takes the maximum value which is H and the complexity is $65\times N\times H$.

Assuming that $PH = H=Q/2$, the total complexity of the proposed method is $2064Q^2+8256Q+262272$ according to Table 5, which is approximated as $O(Q^2)$.

Table 6. Complexity of five methods

Virtual user identification methods	Complexity
The proposed method	$O(Q^2)$
SIS-OPT	$O(3^Q)$
SIS-LF	$O(Q)$
PSP	$O(3^{2Q})$
UDS	$O(Q^2)$

The complexity of the proposed method and that of the reference methods are listed in Table 6. It can be seen that the complexity of the proposed method is higher than that of SIS-LF, lower than that of SIS-OPT and PSP, and in the same order of magnitude with that of UDS.

5. Conclusions

The reliability of virtual user identification and channel security in ad hoc network are threatened by limited user energy. Existed virtual user identification methods have high miss alarm rate and false alarm rate under low SNR and do not consider channel security. Therefore a joint virtual user identification and channel security en/decoding method is proposed in this paper. The proposed encoding method firstly generates transmitter-receiver-based virtual user identification code to resist multi-access interference and inter-symbol interference and then encrypts virtual user identification code with true random sequence to generate orthogonal random security sequence so as to enhance channel security, finally the proposed encoding method divides data packet into 6-bit symbols and maps each symbol with an orthogonal random security sequence to spread spectrum as well as improve transmission efficiency. The proposed decoding method obtains confidences set by processing the received signal with subspace-based method. The virtual users are identified by comparing the confidences with judgment threshold which is an empirical value. Experimental results show that the proposed method obtains 1.6dB E_b/N_0 gains compared with reference methods when miss alarm rate is 10^{-3} and has a lower complexity.

References

[1] WU Weighing and CHEN Kwangcheng. Identification of active users in synchronous CDMA multiuser detection[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(9):1723-1735.

[2] LIN D D and LIM T J. Subspace-based active user identification for a collision-free slotted ad hoc network[J]. IEEE Transactions on Communications, 2004,52(4):612 -621.

[3] PAD P, Soltanolkotabi M, Hadikhanlou S, et al. Errorless codes for over-loaded CDMA with active user detection[C]. IEEE International Conference on Communications, Dresden, Germany, 2009:1-6.

[4] Angelosante D, Biglieri E, and Lops M. Multiuser detection in a dynamic environment—part II: joint user identification and parameter estimation[J] IEEE Transactions on Information Theory, 2009,55(5):2365-2374.

[5] Angelosante D, Biglieri E, and Lops M. Low-complexity receivers for multiuser detection with an unknown number of active users[J]. Signal Processing, 2010,90(5):1486-1495.

[6] Vázquez M A and Míguez J. User activity tracking in DS-CDMA systems[J]. IEEE Transactions on Vehicular Technology, 2013, 62(7):3188-3203.

[7] Zhang Yijin, Shum K W, Wong W S, et al. Binary sequences for multiple access collision channel: identification and synchronization[J]. IEEE Transactions on Communications, 2014, 62(2):667-675.

[8] Tian Shan and Zhang Can. Virtual user identification based on cross-layer design in wireless ad hoc networks[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2009, 26(5):681-687.

[9] Rozovsky R and Kumar P R. Seedex: a MAC protocol for ad hoc networks[C]. Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, Long Beach, CA, USA, 2001:67-75.

[10] Jeong B K, Shim B, and LEE K B. MAP-based active user and data detection for massive Machine-Type Communications[J]. IEEE Transactions on Vehicular Technology, 2018,67(9):8481-8494.

[11] Ahn J, Shim B, and Lee K B.EP-based joint active user detection and channel estimation for massive Machine-Type Communications[J]. IEEE Transactions on Communications, 2019,67(7):5178-5189.

[12] KIM W J, AHN Y J, and SHIM B. Active user detection of machine-type communications via dimension spreading neural network[C]. 2019 IEEE International Conference on Communications, Shanghai, China, 2019:1-6.

[13] RAND. A million random digits with 100000 normal deviates[M]. New York, US, Free Press, 1955:5-404

Kenan Zhang received the B.S. degree from Tianjin University in 2012, and the Ph.D. degree from University of Chinese Academy of Sciences in 2020. He has been an engineer at Beijing Institute of Spacecraft System Engineering since 2020. His research interest includes ad hoc network, wireless communication, multiuser detection and virtual user identification

Xingqian Li received the B.S. and M.S. degrees from Beihang University in 2003 and 2006 respectively. He has been a researcher at Beijing Institute of Spacecraft System Engineering since 2006. His research interest includes the overall design of spacecraft.

Kai Ding received the B.S. degree from Tsinghua University in 2001, and the Ph.D. degree from Institute of Electrics, Chinese Academy of Sciences in 2006. He has been a researcher at Beijing Institute of Spacecraft System Engineering since 2006. His research interest includes wireless communication and satellite communication.

Li Li received the B.S. degree from North China Institute of Science and Technology in 2018, and the M.S. degree from University of Chinese Academy of Sciences in 2021. She has been an engineer at Computer Network Information Center, Chinese Academy of Sciences since 2021. Her research interest includes communications.