Carrier Sense Random Packet CDMA Protocol in Dual-Channel Networks

Chuan-bao DU[1], Hou-de QUAN[1], Pei-zhang CUI[1], Wei LIANG[1,2], Po ZHOU[1], Jian-bin DOU[1,3]

[1] Dept. of Information Engineering, Mechanical Engineering College, 050003, Shijiazhuang, China
[2]Dept. of Automation, Tsinghua University, 100084, Beijing, China
[3]Key Laboratory of Guided Weapons Test and Evaluation Simulation Technology, 714200, Huayin, China

{leopard0306, quanhoude, cuipeizhang}@126.com, lw94245@sina.com, {zhoupo,jianbindou}@126.com

Abstract. *Code resource wastage is caused by the reason that many hopping frequency (FH) sequences are unused, which occurs under the condition that the number of the actual subnets needed for the tactical network is far smaller than the networking capacity of code division networking. Dual-channel network (DCN), consisting of one single control channel and multiple data channels, can solve the code resource wastage effectively. To improve the anti-jamming capability of the control channel of DCN, code division multiple access (CDMA) technology was introduced, and a carrier sense random packet (CSRP) CDMA protocol based on random packet CDMA (RP-CDMA) was proposed. In CSRP-CDMA, we provide a carrier sensing random packet mechanism and a packet-segment acknowledgement policy. Furthermore, an analytical model was developed to evaluate the performance of CSRP-CDMA networks. In this model, the impacts of multi-access interference from both inter-clusters and intra-clusters were analyzed, and the mathematical expressions of packet transmission success probability, normalized network throughput and signal interference to noise ratio, were also derived. Analytical and simulation results demonstrate that the normalized network throughput of CSRP-CDMA outperforms traditional RP-CDMA by 10%, which can guarantee the resource utilization efficiency of the control channel in DCNs.*

Keywords

Spread-spectrum ad hoc network, full-connected cluster, random packet-code division multiple access, multi-access interference, multiuser detector, Poisson distribution

1. Introduction

Wireless ad hoc networks that are widely deployed for tactical communication are mainly constructed by the de-synchronization or synchronization methods. Compared with a de-synchronized network, a synchronized network has many advantages in network interoperability, large networking scale, strong track interference resistance and high throughput. Hence the synchronized network is mainly used in a large-scale tactical environment. On the battlefield, a common tactical network should be divided into a fewer subnets for tactical communication. Since the number of subnets needed in a common tactical network is far smaller than the theoretical networking capacity, a large number of frequency hopping (FH) sequences are unused, which causes serious code resource wastage. Theoretical networking capacity denotes the maximum number of subnets that the network can be divided into, under the condition that the network is orthogonal and synchronized. The theoretical networking capacity is equal to the number of frequency points used in the network. To reduce code resource wastage, dual-channel network (DCN), which consists of one control channel and multiple data channels and employs a hierarchically distributed ad hoc networks based on a fully connected network, was proposed [1]. The network reliability of DCN depends on the anti-jamming capability of the control channel, which is one of the key technologies of DCN design. As a result of advanced channel access and anti-jamming capability, the spread-spectrum ad hoc network technology is introduced into the design of the control channel to enhance the interference resistance [2].

We assume that spread spectrum ad hoc networks is slotted [3], but we do not focus on synchronization. In this type of networks, the nodes are always divided into multiple fully connected networks, which are distinguished from each other through multiple spreading codes [4]. Because of direct-sequence spread spectrum signaling, the receiver in a typical network can distinguish the concurrently received packets overlaying in both the space and time domains. The transmitter or receiver should know the spreading code used for the reference packet. The rule of how to assign a spreading code is the purpose of code assignment. Four categories of spreading-code assignment protocols have been proposed [5–9]: Common-code; Receiver-based; Transmitter-based; Hybrid [5].

Random packet code division multiple access (RP-CDMA) [10], which is a packet-level spread-spectrum multi-access scheme, provides private, connectionless and

uncoordinated random channel access. RP-CDMA also provides a novel code assignment protocol, which is different from the traditional protocols described above. Its packet format consists of a short packet header and a long packet payload. Each header is spread with a common code identical for all nodes, while the payload of each packet is spread with a randomly generated spreading code. Each receiver consists of a header detector and a payload detector. RP-CDMA has been originally applied separately to a centralized station network and a satellite network based on the Aloha system. In these two networks, the receiver always transmits acknowledge packets in another channel because of bi-directional links, which does not cause any collision between the data packet and acknowledge packet [11]. In addition, Kempter et al. applied RP-CDMA to ad hoc networks with simple and flat topology, and they focused on the multiuser detector performance of RP-CDMA, but did not design any MAC protocol that considered the unidirectional link of half-duplexed terminals. T. Mortimer et al. [12] designed a MAC protocol for an ad hoc network with RP-CDMA, but they did not consider the clustered topology or provide the analytical models of spread spectrum ad hoc networks with RP-CDMA.

In this paper, we propose a new MAC protocol called carrier sense random packet CDMA (CSRP-CDMA) to improve the interference resistance and the resource utilization efficiency of the control channel. We provide performance evaluation models for slotted spread-spectrum ad hoc networks by considering intra-cluster and inter-cluster multi-access interferences (MAIs), Additional White Gaussian Noise (AWGN), and packet collisions. Moreover, the performance measures such as packet transmission success probability, network throughput, and the signal interference to noise ratio (SINR) are investigated. Based on the presented models, the effects of spreading gain, network scale, detection capability, and signal propagation distance on network performance are analyzed. Finally, we simulate the proposed protocol in comparison with the existing protocols. The analytical and simulation results demonstrate that, compared to traditional RP-CDMA, the normalized network throughput based on CSRP-CDMA can reach 0.48, which guarantees the resource utilization efficiency of the control channel. The results can be used as the optimal parameter configuration for the design of the control channel.

The rest of the paper is organized as follows. Section 2 describes DCN. The system model is provided in Sec. 3. Section 4 presents CSRP-CDMA protocol. The performance evaluation model is presented in Sec. 5. The analytical and simulation results are discussed in Sec. 6. Finally, Section 7 concludes the paper.

2.   Dual-Channel Networks

Code resource wastage is often caused in the traditional tactical networks by using the method of synchronization networking. Thus, with the orthogonal and synchronized networks as an example (Fig. 1), the group net uses the frequency division networking method to distinguish

from each other. The frequency set in group net no. 1 is $\{f_0, f_1, f_2, \ldots, f_{n-1}\}$, where n is the number of frequency points. The theoretical networking capacity is n under the condition that the network is orthogonal and synchronized. As shown in Fig. 1, there are m sequences (*Seq. 1~ Seq. m*) assigned to m subnets in the group net no. 1, and the other $n - m$ sequences (*Seq. m + 1~ Seq. n*) are unused, which means the frequency points corresponding with these unused sequences are code resource wastage because no radio can use them. Hence, code resource wastage is very severe when m is very small.

DCN is proposed to improve resource utilization efficiency. It uses a hierarchically distributed network structure and its sub-cluster is a fully connected network, which implies all the nodes in a sub-cluster can communicate with each other in one hop distance. The dual-channel structure of a node consists of a control channel and multiple data channels. The control channel is assigned before networking with the same FH sequence to exchange the network management and route control messages, and this FH sequence is fixed until the whole network is dismissed. The data channel will be established when a node pair has the request of data transmission. To transmit data packets, all nodes in the data channel will be assigned with the same idle FH sequence chosen from the idle code resource pool. In brief, each FH sequence is deemed as a frequency-point-varying channel, and the DCN must contain multiple frequency points during each FH slot period. Since a DCN has one single transceiver, its node stays at either control channel or data channel by switching the single transceiver via a time division mechanism. The DCN has the following main merits: 1) the idle code resource can be reused dynamically by any subnet building multiple data channels between communication radio pairs; 2) the inter-cluster communication of traditional networks is realized with the use of extra convertor equipment, but that of DCN can be realized by building a data channel with a special common FH sequence only for the communication radio pairs.

Fig. 2 illustrates the structure of DCN. The solid lines denote the data channel, and the dotted lines denote the control channel. In addition, the virtual backbone network consists of all the gate nodes and subnet-header nodes in the DCN   for inter-cluster communication. Assuming the
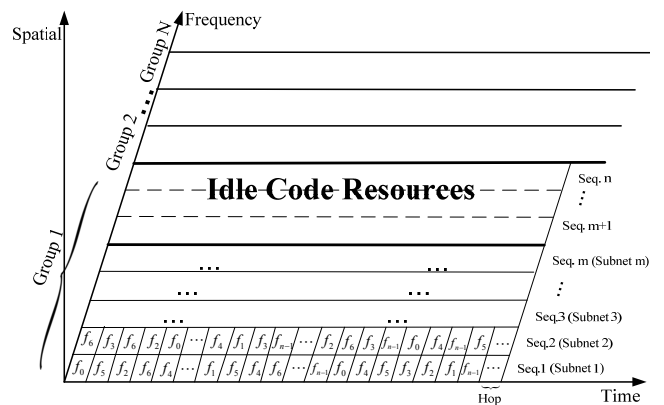

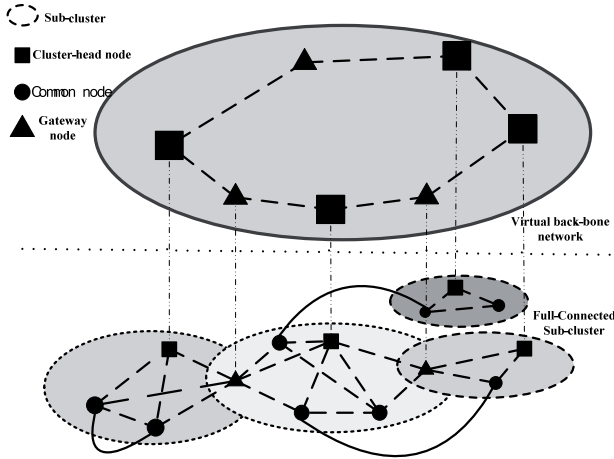**Fig. 1.**   Illustration: Idle code resources.

Fig. 2. Dual-channel networks structure.

Symbol	Explanation
λ_s	Rate of Poisson process
L_h	The length of the packet header
N_h	The spreading gain of packet header
T_h	The header duration
L_d	The length of the packet payload
N_d	The spreading gain of packet payload
T_d	The payload duration
T_p	The packet duration
$Power_t$	The transmitted power of the sending node
$Power_r$	The received power of the receiving node
$\Gamma_j^{(mf)}$	SINR of a packet j at the output of the header detector with MF
$Powerh_j$	Received header power of packet j at the header detector's front-end
$Powerh_{int}$	Total received power of all interference packets at the header detector's front-end
γ_{mf}	SINR threshold of the header detector with MF
γ_{mmse}	SINR threshold of the payload detector with MMSE
$\Gamma_j^{(mmse)}$	SINR of a packet j at the output of the payload detector with MMSE
$E_P[\bullet]$	Expectation of the received power of each interference payload at the payload detector's front-end
$Powerd_j$	Received payload power of packet j at the payload detector's front-end
K	Average number of MAI users at the payload detector's front-end
$Powerd_i$	Received power of the interference packet i at the payload detector's front-end

Tab. 1. Major notation used in system model.

node mobility in the DCN is low, we do not focus on high mobility in this paper. For simplicity, the subnet is called "cluster" instead of "sub-cluster" in the rest of the paper.

3. System Model

In this section, we describe the details of a DCN sys

tem model composed of node distribution model, packet format, signal transmission model and receiver model. The assumptions of the system model are as follows: 1) the whole network is based on slot synchronization; 2) the whole network deploys a hierarchically distributed network structure and each cluster is based on a fully connected network (Fig. 2); 3) packet transmission can be interfered with the collisions, MAI [13] and channel noise. The major notations used in the receiver model are listed in Tab. 1.

3.1 Node Distribution Model and Packet Format

For simplicity, we assume that all nodes are deployed at the designated area in a Poisson random distribution, regardless of the tactical task requirement. During one packet duration, the distribution of sending-node number in Area A follows a Poisson process at rate λ_s. Thus, the probability P_s that the sending-node number k in any cluster during one packet duration is computed as follows:

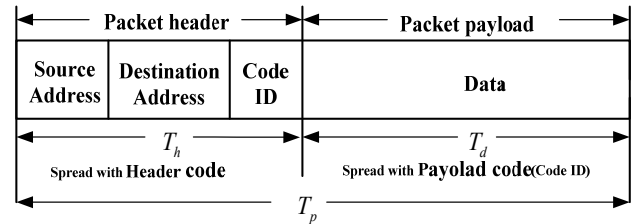$$P_s(k) = \frac{(\lambda_s A)^k e^{-\lambda_s A}}{k!}. \tag{1}$$

Fig. 3. Packet format.

Fig. 3 shows the packet format used for the system. On the assumption that a packet header is only allowed to be sent or received during only one slot duration that is defined as the minimum time unit used for this system. Thus, we set the header duration T_h to one slot. Hence, the duration of the packet payload satisfies

$$T_d = (N_d L_d / N_h L_h) T_h. \tag{2}$$

Thus, the packet length $L_p = L_d + L_h$ bits, the packet duration is $T_p = (1 + N_d L_d / N_h L_h) T_h$.

3.2 Signal Transmission Model

We denote the distance between a sending node and a receiving node as d, the transmitted power of the sending node as $Power_t$, and the received power of the receiving node as $Power_r$. Thus, $Power_r$ is expressed as [14]:

$$Power_r = \begin{cases} C\dfrac{Power_t}{d^n}, & d \geq r \\ Power_t, & d < r \end{cases} \tag{3}$$

where r is the boundary between the near field and the far field, n is the attenuation factor, and C is a constant.

3.3 Receiver Model

Fig. 4 illustrates the receiver structure used for the system. The receiver structure consists of a packet header detector and a packet payload detector. The packet header detector is a single-user matched filter (MF), while the packet payload detector is a multiuser detector such as MF [15], Decorrelator [16], Minimum Mean Square Error (MMSE) [17], and Successive Interference Cancellation (SIC) [18].
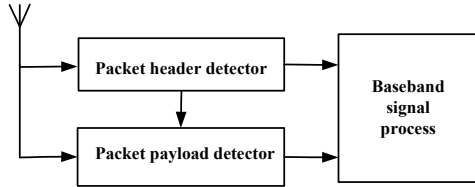

Fig. 4.   Receiver structure.

In our work, we use a single-user MF as the packet header detector and a MMSE as the packet payload detector. When multiple packet payloads coming from different source nodes arrive at the receiver simultaneously, they can be recovered successfully by the packet payload detector using multiple payload spreading codes. Because the packet header and the packet payload use different spreading codes, the detection of the packet header is not interfered with the packet payload. However, the detection of packet payload depends on the multiuser detection capability when there is too much interference from other packet payloads. Therefore, the multiuser detection capability constrains the system's anti-MAI performance. Furthermore, the packet header collision, which is caused by multiple headers arriving at the receiver during the same slot duration, is the only potential packet collision, because packet headers in a cluster use the same spreading code.

Generally, since the ratio of header length to payload length is very small, the channel load of the packet header is extremely slight which means the probability of header collision is very low. We assume that the packet header detector uses a single-user matched filter, then SINR $\Gamma_j^{(mf)}$ of packet j at the output of header detector is calculated as

$$\Gamma_j^{(mf)} = \frac{Powerh_j}{\sigma^2 + \frac{1}{N_h} Powerh_{int}} \tag{4}$$

where σ^2 is the normalized variance of AWGN. Then packet j will be detected successfully if $\Gamma_j^{(mf)} \geq \gamma_{mf}$.

Then we assume that the packet payload detector is an MMSE multiuser detector and that the threshold of MMSE is γ_{mmse}. Similarly, the payload of packet j will be detected successfully when the SINR $\Gamma_j^{(mmse)}$ of packet j satisfies $\Gamma^{(mmse)} \geq \gamma_{mmse}$. $\Gamma_j^{(mmse)}$ can be expressed as follows [16]:

$$\Gamma_j^{(mmse)} = \frac{Powerd_i}{\sigma^2 + \frac{KE_P\left[I\left(Powerd_i, Powerd_j, \Gamma_j^{(mmse)}\right)\right]}{N_d}} \tag{5}$$

where $E_P[\bullet]$ is the expectation of the received power of each interference packet payload. Here, we have

$$I\left(Powerd_i, Powerd_j, \Gamma_j^{(mmse)}\right) \equiv \frac{Powerd_i \cdot Powerd_j}{Powerd_j + Powerd_i \cdot \Gamma_j^{(mmse)}} \tag{6}$$

4. CSRP-CDMA Protocol

This section provides the details of CSRP-CDMA. Based on a reported MAC protocol [12], CSRP-CDMA is mainly added with a packet-segment-based acknowledgement policy (PSAP) and carrier sensing random packet mechanism (CSRPM). For simplicity, we neglect the other parts of CSRP-CDMA, which are similar to RP-CDMA [12]. Thus, we focus on PSAP and CSRPM.

CSRP-CDMA has the same packet format as RP-CDMA, which consists of a packet header and a packet payload. The packet header is encoded with a common code used for all nodes to transmit payload code ID placed in the header, while the packet payload is encoded with a randomly-generated payload code to transmit data portion.

The Eventual Acknowledgement policy [12] eventually acquires the receiving node to send accumulated acknowledgments (ACKs) when the receiver is idle. Because multiple transmission tasks in a cluster is very common, the opportunity of sending ACKs is not guaranteed, which can decrease the probability of packet transmission success. Hence, CSRP-CDMA uses PSAP to solve this problem above. In PSAP, the sending node divides a time frame into multiple packet segments, and waits for acknowledgements before the subsequent transmission. The receiving node when idle will send accumulated ACK packets, which are encoded with the source payload spreading code. PSAP not only guarantees the efficiency and reliability of the packet transmission, but also maintains the frame design regulations of the upper layer adapted to the existing systems.

Since the system utilizes the slotted synchronization, the length of the packet header is equal to that of one slot, and the packet header (PH) would be transmitted only at the beginning of a slot. Each node has a neighbor status table (NST) in its own register. The node only stays at send-status (SS) or receive-status (RS). When the node is transmitting a packet segment, the status is called SS; otherwise, it is called RS.

Each packet header should contain the source address (SA), destination address (DA), and the end identifier of the packet segment (PEID) or time frame (TEID). The node at RS can monitor the packet headers of neighbor nodes (NNs) and then calculate which NN will transmit packet in the next packet duration. According to these results, the node can confirm whether the destination node (DN) stays at RS if it wants to transmit packets. Then the node can decide to transmit packets immediately when the DN stays at RS, or to postpone packet duration for sensing status change of the DN again. The steps of CSRPM are as

follows (Fig. 5):

- Step 1: Prepare to send a packet. Look up the NST for the status of DN;

- Step 2: Decide the status of DN: if it is RS, go to step 9, or else, go to step 3;

- Step 3: Sense and demodulate PH;

- Step 4: Decide whether the PH is sent to DN: if yes, go to step 5, otherwise, go to step 8;

- Step 5: Decide whether the PEID or TEID is true: if yes, go to step 6, otherwise, go to step 3;

- Step 6: Wait for the next payload duration;

- Step 7: Update the related node status in NST, and then go to step 9;

- Step 8: Decide whether the PH comes from DN: if not, delay one slot and go to step 7, or otherwise, go to step 3;

- Step 9: Send this packet.

Begin (Prepare to send packet)
  Look up NST to judge whether the DN is RS or not?
    If the DN is, then go to send packet; if not, sense PH;
  Sense PH and decide whether the PH comes from the DN?
    If it does, then decide whether the identifier of PEID or TEID is true?
      If it is, wait for the next payload duration;
      If not, return to sense PH;
    If not, then decide whether PH is related to DN?
      If it is, delay one slot;
      If not, return to sense PH;
  Update NST;
  Send the packet;
END

Fig. 5. Algorithm of the CSRP mechanism.

5. Performance Analysis

In this section, we calculate the expressions of packet transmission probability, normalized network throughput, and SINR. We assume that all nodes in the network are homogenous, and $Power_t$ denotes the transmitted power. The DCN consists of U fully connected clusters ($U \leq 2^{N_h} - 1$), and each cluster utilizes a unique header spreading code to transmit intra-cluster headers. The header spreading codes are chosen from the code set $\{C_{h1}, C_{h2}, ..., C_{hU}\}$ at the networking phase. All packet payloads in the DCN are spread with the payload spreading codes generated randomly by the same code generator, and these codes are generated in the set $\{C_{d1}, C_{d2}, ..., C_{dM}\}$, $M = 2^{N_d} - 1$. In addition, the header spreading code is fixed until its cluster ends, while the payload spreading code used for each packet payload is generated randomly with an equal chance every time. Furthermore, all nodes are distributed uniformly and independently, and the number of the sending nodes follows the Poisson distribution. The major notations used in performance analysis are in Tab. 2.

Symbol	Explanation
P_p	Probability of packet transmission success
P_h	Probability of packet header detection success
P_d	Probability of packet payload transmission success
P_{hc}	Probability of header detection success affected by the collision
P_{hi}	Probability of header detection success affected by interference signals
$P_s(k_c)$	Probability of the sending-node number k_C in cluster area S_C
$f(d)$	Probability density function of distance d_i between the sending node i and $Node_R$
$Powerh_{int}$	Total interference received power at the header detector's front-end
$E\left[d_i^{-n}\right]$	Expectation of signal transmission loss of all interference signals arriving at node $Node_R$
$E\left[d_T^{-n}\right]$	Expectation of transmission loss of the reference signal from node $Node_T$
$Powerd_{int}$	Total interference received power at the payload detector's front-end
$P_{codecol}(k)$	Probability that the payload spreading code used for the reference packet is different from the codes used for other packets

Tab. 2. Major notations used in performance analysis.

5.1 Packet Transmission Probability

In slotted ad hoc networks, a packet accesses channels randomly, and is only transmitted at the beginning of a slot. The packet transmission will fail following the failure in the packet header transmission or the payload transmission. Hence, the success of packet transmission is defined as both packet header detection success and packet payload transmission success. Then the packet transmission probability is expressed as

$$P_p = P_h P_d \quad . \tag{7}$$

First, each cluster transmits its packet headers by using a unique header spreading code, which is used to distinguish the header from those of other cluster. Therefore, the reference packet header will not collide with other cluster headers. However, it still suffers from the MAIs of packet payloads transmitted near the receiver. Second, the reference packet header may collide with other headers in the same cluster since they use the same header spreading code. Thus, the probability P_h of the packet header detection success is expressed as

$$P_h = P_{hc} P_{hi} \quad . \tag{8}$$

The distribution of MAI nodes near the reference receiving node $Node_R$ is shown in Fig. 6, where $Node_T$ is the reference sending node. We denote the signal propagation distance as R, and the cluster range as R_c, and the radius of MAI range R_{max} with the assumption that no interference occurs when the interference node is outside the MAI range. In the packet duration, the probability of the sending-node number k_c in the cluster area S_C is $P_s(k_c)$ according to (1). Furthermore, we assume that the header of the reference packet occurs in the first slot of the packet duration, so that the header will be detected successfully only when the
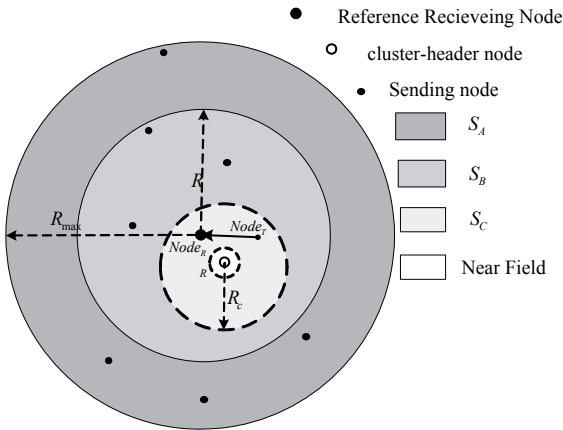
Fig. 6. Distribution of MAI nodes nearby the reference receiving node.

other $k_c - 1$ headers occur in other slots. Hence,

$$P_{hc} = \sum_{k_c=1}^{+\infty} \left(P_s(k_c) \frac{(T_p-1)^{(k_c-1)}}{T_p^{(k_c-1)}} \right) . \quad (9)$$

As shown in Fig. 6, the MAI interference area S_{ABC} of $Node_R$ can be expressed as $S_{ABC} = S_A + S_B + S_C = \pi R^2_{\max}$. Fig. 7 shows how the MAIs of other packets affect the reference packet headers. The Poisson probability density function (PDF) of the sending-node number k is $P_s(k)$ at rate λ_s according to (1).

The channel attenuation model indicates that the signal strength is attenuated badly as the distance increases. In addition, the locations of the sending nodes in the area obey a uniform and independent distribution. Therefore, we assume that the distance d_i between the sending node i and $Node_R$ is within the variable set $\{d_1, d_2, \ldots, d_k\}$, and its PDF of which is expressed as

$$f(d) = \begin{cases} \dfrac{2d}{R^2_{\max}} & 0 \le d \le R_{\max} \\ 0 & else \end{cases} . \quad (10)$$

The derivation of (10) comes from $(\pi d^2)/(\pi R^2_{\max})$, which is the cumulative distribution function (CDF) of the distance d_i.
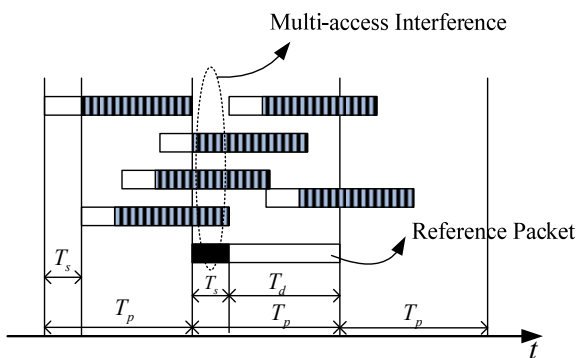

Fig. 7. Diagram of the packet header suffer from MAI.

With (3), the total interference received power $Powerh_{int}$ at the header detector's front-end can be computed as

$$Powerh_{int} = C(k-1) Power_t E\left[d_i^{-n} \right] . \quad (11)$$

For (11), there is no sending node in the near field with the range r, because the near field range is too small to be considered under very high frequency (VHF) tactical scenarios. Thus, we only focus on the far field. Therein, $E[d_i^{-n}]$ is the expectation of signal transmission loss of all interference signals arriving at $Node_R$. According to (10), $E[d_i^{-n}]$ is calculated as

$$E\left[d_i^{-n} \right] = \frac{2}{(n-2)(R_{\max})^2} \left| \frac{1}{r^{n-2}} - \frac{1}{(R_{\max})^{n-2}} \right| . \quad (12)$$

Since $Node_T$ must be in the reference cluster area S_c, then $0 < d_T \le R$. Similarly, the expectation $E[d_T^{-n}]$ of the transmission loss of the reference signal from $Node_T$ is computed as

$$E\left[d_T^{-n} \right] = \frac{2}{(n-2)R^2} \left| \frac{1}{r^{n-2}} - \frac{1}{R^2} \right| . \quad (13)$$

According to (1), (4), (11), (12) and (13), the probability P_{hi} of header detection success under interference is computed as

$$P_{hi} = P\left(Powerh_{int} \le C \frac{N_h E\left[d_T^{-n} \right] Power_t}{\gamma_{mf}} - \sigma^2 \right)$$
$$= P_s\left(k < \left\lfloor \frac{C \dfrac{N_h E[d_T^{-n}] Power_t}{\gamma_{mf}} - \sigma^2}{C \cdot Power_t E[d_i^{-n}]} + 1 \right\rfloor \right) = \sum_{k=1}^{K_{hmax}} P_s(k) . \quad (14)$$

In (14), K_{hmax} can be calculated as

$$K_{hmax} = \left\lfloor \frac{C \dfrac{N_h E[d_T^{-n}] Power_t}{\gamma_{mf}} - \sigma^2}{C \cdot Power_t E[d_i^{-n}]} + 1 \right\rfloor . \quad (15)$$

The reference payload suffers from the MAIs of other packets in the MAI area, but it will collide with other payloads if they use the same spreading code. $Node_T$, which the reference payload comes from, must be within the reference cluster area S_c. As previously described, the PDF of the sending-node number k in the MAI area S_{ABC} is $P_s(k)$. From (3) and (5), $Powerd_{int}$ can be computed as

$$Powerd_{int} = (k-1) E_p\left[I\left(Powerd_i, Powerd_j, \gamma_{mmse} \right) \right]$$
$$= (k-1) \frac{\left(CE\left[d_i^{-n} \right] Power_t \right) \cdot \left(CE\left[d_T^{-n} \right] Power_t \right)}{\left(CE\left[d_T^{-n} \right] Power_t \right) + \left(CE\left[d_i^{-n} \right] Power_t \right) \cdot \gamma_{mmse}} . \quad (16)$$

Like P_{hi}, the probability P_d of payload transmission success with the presence of interference is expressed as

$$P_d = P\left(Powerd_{int} \le \left(\frac{Powerd_j}{\gamma_{mmse}} - \sigma^2 \right) N_d \right) = \sum_{k=1}^{K_{dmax}} \left(P_s(k) P_{codecol}(k) \right) \quad (17)$$

In (17), K_{dmax} can be computed as

$$K_{\text{dmax}} = \left\lfloor \frac{\left(C \dfrac{E\left[d_T^{-n} \right] Power_t}{\gamma_{mmse}} - \sigma^2 \right) N_d}{C \dfrac{E\left[d_i^{-n} \right] \cdot Power_t}{1 + CE\left[d_T^{-n} \right] \gamma_{mmse}} + 1} \right\rfloor . \qquad (18)$$

In (17), $P_{codecol}(k)$, the probability that the payload spreading code used for the reference packet is different from the codes used for other packets, is calculated as

$$P_{codecol}(k) = \left(1 - \frac{1}{2^{N_d} - 1} \right)^{k-1} . \qquad (19)$$

5.2 Normalized Network Throughput

The network load G is defined as the average number of packets generated by the reference cluster in one packet duration. Thus,

$$G = \lambda_s S_C = \pi \left(\frac{R}{2} \right)^2 \lambda_s . \qquad (20)$$

In (20), S_c is the area of the reference cluster, and λ_s is the Poisson probability density of sending-node number in the cluster.

The network throughput S is defined as the average number of the successfully received packets in one cluster, and it satisfies $S = GP_p$ [19]. Considering that the spread-spectrum networks occupy extra spectrum resources, we introduce a spread gain into S during the network performance evaluation. Hence, the normalized network throughput S_{normal} can be defined as

$$S_{normal} = S / N_d . \qquad (21)$$

5.3 SINR

The works above indicate that the expectation of sending-node number in the MAI area S_{ABC} of $Node_R$ is calculated as

$$E[k] = S_{ABC} \lambda_s = \pi R_{\max}^2 \lambda_s . \qquad (22)$$

Using (12) and (22), we can obtain the mean power $E[I]$ of interference signals at the receiver's front-end as follows:

$$E[I] = CE[k] E\left[d_i^{-n} \right] Power_t + \sigma^2 . \qquad (23)$$

Therefore, the signal interference to noise ratio $SINR_m$ is computed as

$$SINR_m = \frac{CE\left[d_T^{-n} \right] Power_t}{CE[k] E\left[d_i^{-n} \right] Power_t + \sigma^2} . \qquad (24)$$

According to (24), SINR is affected by the transmission distance, sending-node distribution density, and attenuation factor.

6. Numerical and Simulation Results

In this section, we analyze the capability of the header detector, the capability of the payload detector, S_{normal} and $SINR_m$. In addition, we compare CSRP-CDMA and traditional RP-CDMA on OPNET 14.5. The network scenarios considered are typical tactical VHF clustered ad hoc networks. Thus, the network parameters in this section are signal frequency $f = 80$ MHz, attenuation factor $n = 4$, signal transmission range $R = 5$ km, and near field range $r = 300/(2\pi f)$. Here, the near field is negligible.

6.1 Maximum Packet Detection Capability

We define the maximum detection capability as the maximum number of intra-cluster interference packets arriving at a receiver that will not subject the reference packet transmission to failure. This definition also implies the maximum number of concurrent packets that are recovered successfully by the detector. The maximum detection capabilities of the header detector and payload detector vs. spread-spectrum gain at different SNRs are shown in Fig. 8. The header detection capability depends on N_h and the payload detection capability is limited by N_d.
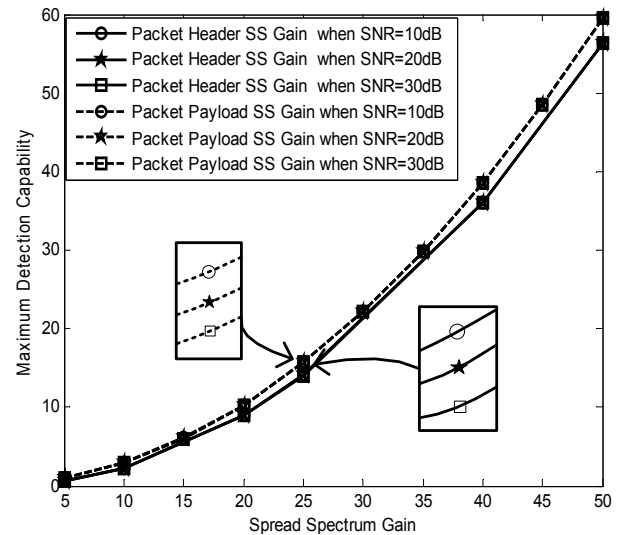

Fig. 8. Detection capabilities of header detector and payload detector.

The results show that the maximum number of received packets increases rapidly as the spreading gain grows. Moreover, the SNR of the detector's front-end affects the detection capability, but not significantly, because the AWGN is very small in comparison with MAI. Furthermore, the capability of the header detector is similar with that of the payload detector when they have the same spread gain, although the payload detection capability is slightly higher.

6.2 Network Performance Analysis

Fig. 9 shows the curves of packet transmission probability P_p and normalized network throughput S_{normal} vary-
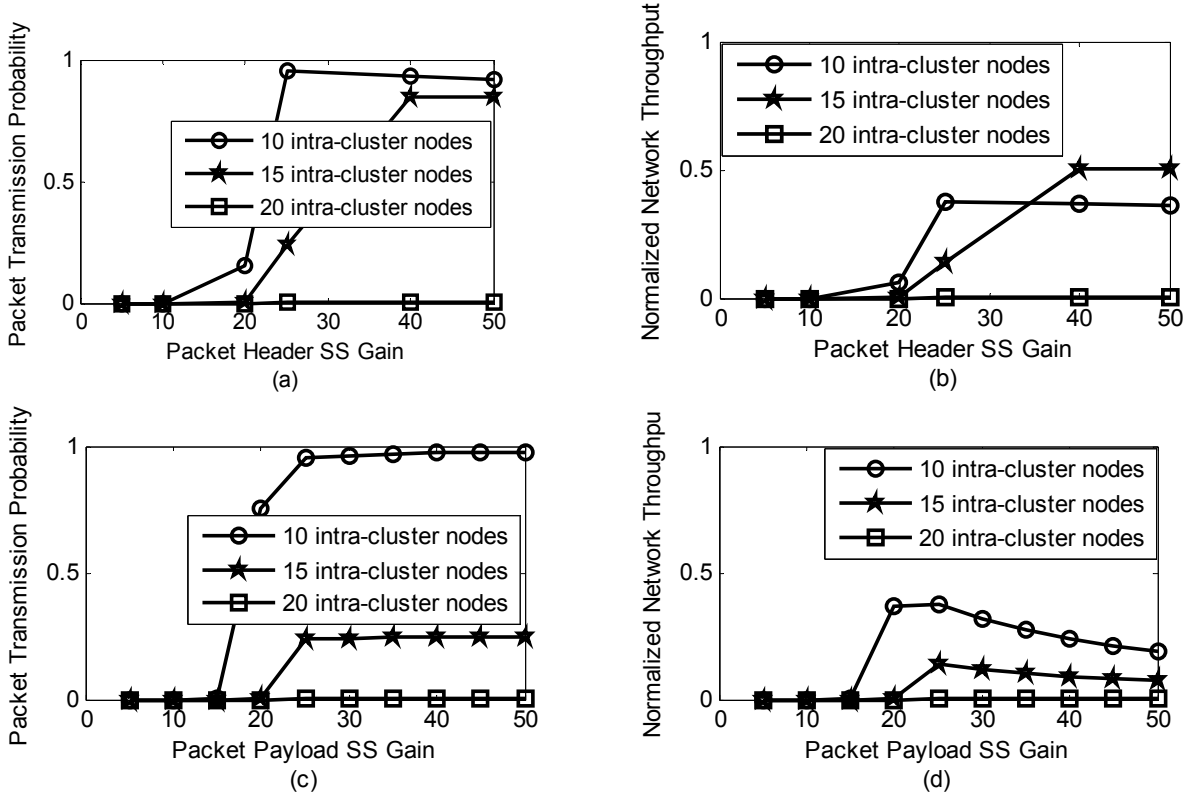
Fig. 9. Network performance varying header spread-spectrum gain and payload spread-spectrum gain for different network scale.
(a) P_p vs. N_h, (b) S_{normal} vs. N_h, (c) P_p vs. N_d, (d) S_{normal} vs. N_d.

ing header spreading gain N_h and payload spreading gain N_d, respectively. Based on previous works, the parameters in Fig. 9 are $SNR = 10$ dB, the payload to header ratio $PHR = 200$, as well as $N_d = 25$ (Fig. 9a and b), and $N_h = 25$ (Fig. 9c and d). Hence, we conclude that the payload detection capability is about 15 (Fig. 9a and b), and the header detection capability is about 15 (Fig. 9c and d).

All curves in Fig. 9(a) and (b) first increase and then maintain at a certain level, except the curve with 20 intra-cluster nodes. P_p and S_{normal} are optimized when the cluster contains 10 sending nodes. On the curve with 20 intra-cluster nodes, P_p and S_{normal} are close to zero when the network loads are far beyond the receiver capability. Hence, aiming at the curve with 10 intra-cluster nodes in Fig. 9 (a) and (b), we find that $N_h > 25$ cannot affect P_p or S_{normal}, because the network performance is limited by both the header detection capability and the payload detection capability.

Similarly, on the curve with 10 intra-cluster nodes (Fig. 9c and d), P_p and S_{normal} increase when $N_d < 25$, and S_{normal} decreases when $N_d > 25$. This is because the increase of N_d occupies more spectrum band, which reduces S_{normal} when N_d exceeds the value required by the network load. We further derive that the network performance depends on the header and payload detection capabilities.

Fig. 10 shows the network performance varying different PHR. The parameters are $N_h = 25$, $N_d = 25$, and $SNR = 10$ dB. Clearly, P_p and S_{normal} increase rapidly when $PHR < 100$, but stop increasing when $PHR > 150$ (Fig. 10a

and b). Thus, we conclude that the header should be much shorter than the payload in order to effectively reduce the collision between multiple headers.
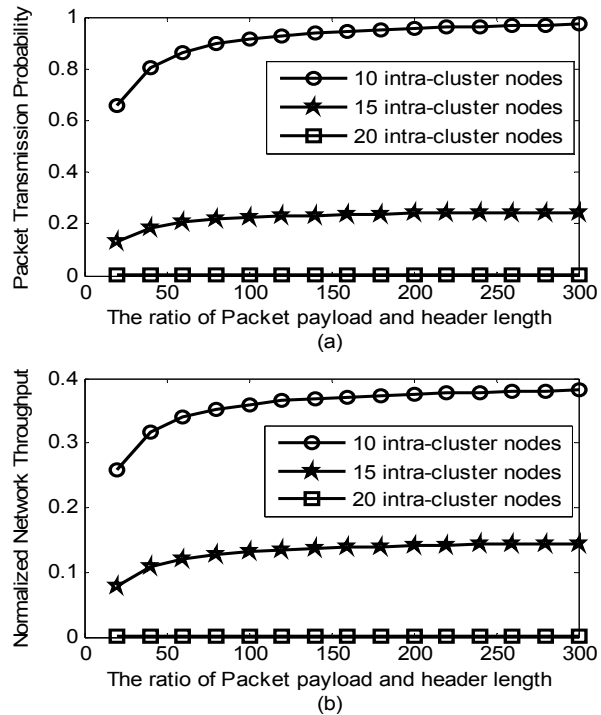

Fig. 10. Network performances varying the ratio of Packet payload and header for different network scale. (a) P_p vs. PHR. (b) S_{normal} vs. PHR.
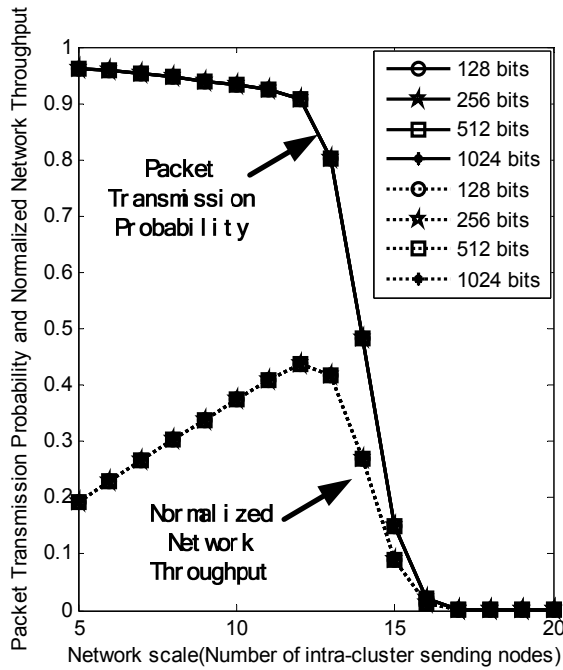
Fig. 11. Packet transmission success probabilities and normalized network throughput different varying network scales.

Fig. 11 shows the performance measures such as P_p and S_{normal} affected by the influence of packet size. The parameters in Fig. 11 are as follows: $N_h = 25$, $N_d = 25$, and $SNR = 10$ dB, and $PHR = 200$. Obviously, we can derive that the packet size does not affect the network performance. This is because each packet is transmitted in a private channel independently by using a unique payload spreading code. Moreover, P_p is higher and S_{normal} increases when the network scale is small, while they both decrease rapidly when the network scale exceeds the detection capability of the receiver.

6.3 SINR

Fig. 12 illustrates the curves of SINR vs. network scales. The parameters in Fig. 12 are $N_h = 25$, $N_d = 25$, and
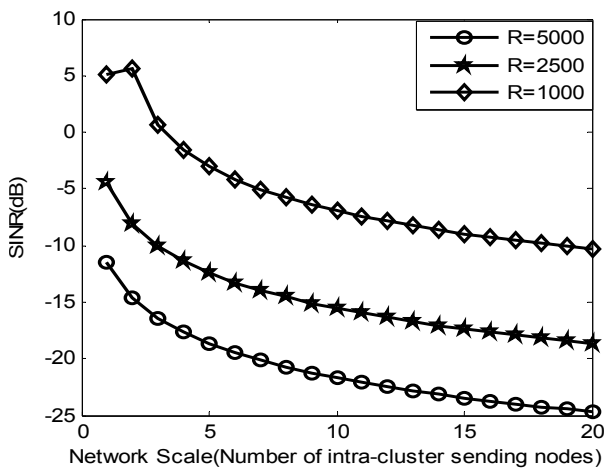

Fig. 12. SINR varying network scale.

$SNR = 10$ dB, and $PHR = 200$. Clearly, SINR decreases when the network scale grows independent of R. It is because SINR is affected by the MAI signals arriving at the receiver rather than AWGN, and obviously, the MAI is more severe as the network scale grows. Moreover, R affects SINR largely, because the MAI signals arriving at the receiver become small as R decreases. Hence, we can adjust the transmitted power to keep R for lower MAIs.

6.4 Comparison between CSRP-CDMA and Traditional RP-CDMA

Because the PSAP and CSRPM of CSRP-CDMA are based on the traditional RP-CDMA protocol [9], Fig. 13 shows the throughputs of both CSRP-CDMA and RP-CDMA vs. network scale. The parameters in Fig. 13 are $SNR = 10$ dB and $PHR = 200$. Under the same condition, the throughput curve of CSRP-CDMA is similar with that of RP-CDMA, but CSRP-CDMA has a higher performance, because they have similar packet detection capability and different packet exchanging processes. When the network load is lower than the receiver capability, the network throughput is close to the network load, so S_{normal} decreases as header and payload spread-spectrum gains grows. Moreover, when both gains are 25, S_{normal} is optimal for the performance requirement of the DCN with 10 intra-cluster sending nodes. The maximum S_{normal} of CSRP-CDMA generally outperforms the traditional RP-CDMA by 10%.
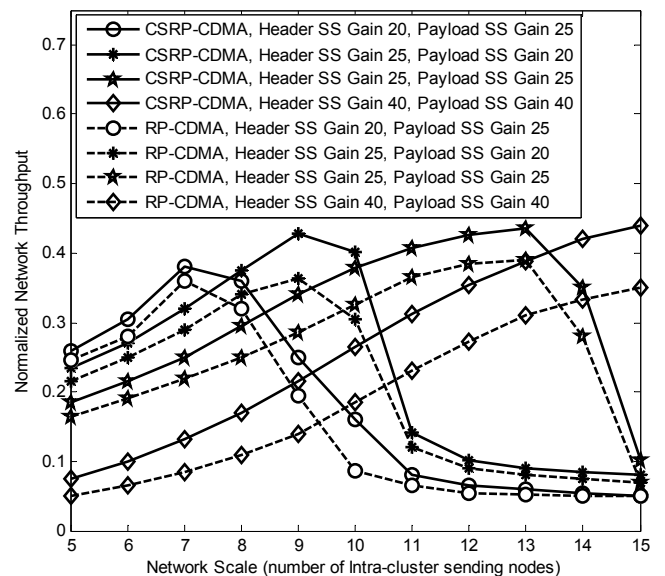

Fig. 13. Throughput of both CSRP-CDMA and RP-CDMA varying different network scales.

7. Conclusions and Futures

We proposed a CSRP-CDMA protocol to improve the control channel anti-jamming capability of a DCN. In CSRP-CDMA, the PSA policy and CSRP mechanism are presented. Considering the combination of packet header collisions, channel noise, as well as intra-cluster and

inter-cluster multi-access interference, we obtained the performance analytical evaluation models for slotted spread-spectrum ad hoc networks based on CSRP-CDMA. The analytical and simulation results are listed below.

1) The packet reception capability depends on both spreading gain and multiuser detector, and the network scale and packet reception capability should be well matched to optimize the network throughput. 2) Compared with AWGN, the MAIs from sending nodes near the receiver affect the network performance significantly. 3) The parameter configuration can be optimized from the evaluation models for DCN design. 4) A compromise is needed between MAI and the requirements of cluster coverage to improve the network throughput by adjusting the transmitted power. 5) CSRP-CDMA outperforms the traditional RP-CDMA by 10% when both header and payload spread-spectrum gains are 25. Hence, CSRP-CDMA is significant in the interference resistance of control channel of DCNs. Further research is needed to extend CSRP-CDMA into the DCNs with high mobility, where an important goal is to improve the interference resistance of control channel under the high mobility.

Acknowledgment

References

[1] DU, C., QUAN, H., CUI, P., WANG, X. A routing protocol for utilizing code resources in tactical ad hoc networks with a single transceiver. *WSEAS Transact. on Communications*, 2014, vol. 13, no. 5, p. 298–308. Available at: http: //www.wseas.org /multimedia/journals/communications/2014/a225704-327.pdf

[2] CHNAG, G., TENG, W., CHEN, H., SHEU, J. Novel channel-hopping scheme for cognitive radio networks. *IEEE Transactions on Mobile Computing*, 2014, vol. 13, no. 2, p. 407–421. DOI:10.1109/TMC.2014.2356475

[3] SUN, S. D., NIE, J. N. Performance comparisons between slotted and un-slotted spread spectrum ad hoc networks. In *Proc. of International Conference on Wireless Communications and Signal Processing*. Nanjing (China), 2009, p. 8–15. DOI: 10.1109/WCSP.2009.5371705

[4] SUN, S. D., NIE, J. N. Performance of spread spectrum ad hoc networks based on Markov chain model. *Journal of Applied Sciences - Electronics and Information Engineering*, 2008, vol. 26, no. 6, p. 562–568. DOI: 10.3969/ j.issn.0255-8297.2008.06.003 [in Chinese]

[5] PNG, K. B., PENG, X. M. Mobility-based interference cancellation scheme for BS-IFDMA systems with optimum code assignment. *IEEE Transactions on Vehicular Technology*, 2013, vol. 62, no. 5, p. 2105–2117. DOI: 10.1109/TVT.2013.2238959

[6] TRAGOS, E. Z., ZEADALLY, S., FRAGKIADAKIS, A. G., SIRIS, V. A. Spectrum assignment in cognitive radio networks: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2013, vol. 15, no. 3, p. 1108–1135. Available at: http:// mm.aueb.gr/publications/2013-spectrum_assignment-surveys.pdf

[7] FYHN, K., JENSEN, T. L., LARSEN, T. Compressive sensing for spread spectrum receivers. *IEEE Transaction on Wireless Communications*, 2013, vol. 12, no. 5, p. 2334–2343. DOI: 10.1109/TWC.2013.032113.120975

[8] ZHONG, Z., ZHANG, L., JIANG, P., WU, H. Blind dispreading of short-code DS-CDMA signals with Bayesian techniques. *Journal of Communications*, 2012, vol. 7, no. 12, p. 928–937. DOI: 10.4304/jcm.7.12.928-937

[9] D'AMOURS, C. Parity bit selected spreading sequences: a block coding approach to spread spectrum. *IEEE Communications Letters,* 2005, vol. 9, no. 1, p. 16–18. DOI: 10.1109/LCOMM.2005.01034

[10] SCHLEGEL, C., KEMPTER, R., KOTA, P. A novel random wireless packet multiple access method using CDMA. *IEEE Transaction on Wireless Communication*, 2006, vol. 5, no. 6, p. 1362–1370. DOI: 10.1109/TWC.2006.1638657

[11] KEMPTER, R. Modelling and evaluation of throughput, stability and coverage of RP-CDMA in wireless networks. *Ph.D. Dissertation*. Utah University, Alta, Canada, 2006. Available at: http://www.researchgate.net/profile/R_Kempter/publication/34688 298_Modeling_and_evaluation_of_throughput_stability_and_cove rage_of_RP-CDMA_in_wireless_networks_/links/542d7cac0cf29 bbc126d34c7.pdf?inViewer=true#pdfjs.action=download

[12] MORTIMER, T., HARMS, J. A mac protocol for multi-hop RP-CDMA ad hoc wireless networks. In *IEEE ICC 2012: Proceedings of Ad Hoc and Sensor Networking Symposium*. Ottawa (ON, Canada), 2012, p. 424–429. DOI: 10.1109/ICC.2012.6364359

[13] INALTEKIN, H. Gaussian approximation for the wireless multi-access interference distribution. *IEEE Transactions on Signal Processing*, 2012, vol. 60, no. 11, p. 6114–6120. DOI: 10.1109/TSP.2012.2212014

[14] CHEN, X., CHEN H., ZHENG, L. Analysis of anti-MAI for CDMA-based ad hoc networks. *Journal of Shanghai University (Natural Sciences)*, 2006, vol. 12, no. 5, p. 441–445. [in Chinese] DOI: 1007-2861(2006)05-0441-05

[15] TSE, K., TSE, D. Effective interference and effective bandwidth of linear multiuser receivers in asynchronisation CDMA systems. *IEEE Transactions on Information Theory*, 2000, vol. 46, p. 1426-1447. Available at: http://citeseerx.ist.psu.edu/viewdoc/ download;jsessionid=3667EF88EF1A3ED2FCD146A7F7BC00C2 ?doi=10.1.1.36.8697&rep=rep1&type=pdf

[16] TSE, D. N. C., HANLY, S. V. Linear multiuser receivers: effective interference, effective bandwidth and user capacity. *IEEE Transactions on Information Theory*, 1999, vol. 45, p. 641–657. DOI: 10.1109/18.749008

[17] BURNASHEV, M. V., SCHLEGEL, C. B., KRZYMIEN, W. A., SHI, Z. Analysis of the dynamics of interference cancellation in interactive decoding. *Problems of Information Transmission*, 2004, vol. 40, no. 4, p. 297–317. DOI: 10.1007/s11122-004-0001-3

[18] SCHLEGEL, C. CDMA with partitioned spreading. *IEEE Communications Letters*, 2007, vol. 11, no. 12, p. 913–915. DOI: 10.1109/LCOMM.2007.070349

[19] GHANBARINEJAD, M., SCLEGEL, C., GBURZYNSKI, P. Adaptive probabilistic medium access in MPR-capable ad-hoc wireless networks. In *The IEEE Global Telecommunications Conf.* Honolulu (Hi, USA), 2009, p. 212–220. Available at: http: //citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.151.3976&re p=rep1&type=pdf

About the Authors …

Chuan-bao DU (corresponding author) was born in Xi'an, China in July 1987. He received his B.E. degree in Dept. of Communication Engineering from Xi'dian University in

2009, received his M.E. degree in Dept.of Information from Mechanical College in 2011. His research interests include wireless communication.

Hou-de QUAN was born in Dalian, China in 1963. He received his PhD degree from Northwestern Polytechnical University, China in 2008. Now he is a professor in Dept. of Information of Mechanical College. His research interests include information and communication engineering.

Pei-zhang CUI was born in Changzhi, China in 1974. He received his B.E. degree from Mechanical College, China in 1996, and his M.E. degree from the 54th Research Institute of CETC, China in 2005. His research interests include information and communication engineering.

Wei LIANG is a Ph.D candidate in the Dept. of Automation of Tsinghua University, China in 2013. Now his research interests are computer science and communication engineering.

Po ZHOU is a lecturer of the Dept. of Information Engineering, Mechanical Engineering College, China. Now his research interests are wireless communication and computer science.

Jian-bin DOU was born in Xianyang, China in 1986. He received his M.E. degree from Mechanical College in 2012. Now his research includes guided weapons tests and evaluation simulation.