Message Broadcast Using Random Relaying of Partitioned MDS Codeword Blocks over Random Error Channels

Shuji Kobayashi, Katsumi Sakakibara, and Jumpei Taketsugu

***Abstract*—Broadcast of a message to nodes in a network is one of elementary but inevitable techniques in wireless ad-hoc and sensor networks. In this paper, we apply the protocol, which the authors proposed for cooperative multi-hop relay networks, to message broadcast over random error channels. Performance is evaluated in terms of the delivery ratio by means of computer simulations. The proposed protocol utilizes an MDS code and a relay node randomly transfers one of partitioned codeword blocks rather than the original message. We suppose a network of square-lattice topology as a preliminary example. Numerical results show that the significant performance improvement can be achieved, in particular, if a relay node can make use of previously received erroneous codeword blocks in the decoding procedure of the MDS code.**

***Index Terms*—Broadcast, communications, Delivery ratio, MDS codes, Random error channels**

I. Introduction

MESSAGE broadcast is a common scenario in wireless ad-hoc and sensor networks. For example, in the AODV (Ad-hoc On-demand Distance Vector) routing protocol, RREQ (Route-Request) messages should be properly broadcast in order to find a route to the destination [1]. When we deliver a message to all the nodes in a network, ``flooding'' is the most simple and basic mechanism [2]. In the flooding mechanism, every relay node transfers the message, upon its first reception, to nodes within its transmission range. Performance of the flooding mechanism has been investigated, for example, from the viewpoint of the connectivity among nodes in conjunction with the percolation theory [3]–[6]. In [3], the probability of survivability of the flooding is discussed. In [4], the forwarding probability at a node in the flooding is evaluated on the assumption that every node knows the number of its own neighboring nodes. Raman and Gupta investigated performance tradeoffs in terms of latency and energy consumption in percolation-based broadcast protocols [5]. In [6], the authors established the conditions for full connectivity in a network graph, based on the results obtained from bond percolation in a two-dimensional lattice.

In wireless ad-hoc networks employing the flooding, it is usual that a message can reach to a relay node through one or more routes. In such a case, multi-route diversity can favorably achieve performance improvement by means of cooperative transmission techniques [7]. The probability of successful broadcast at a relay node which receives two or more copies of the message to be transferred can be improved, since it suffices for a relay node to receive at least one copy correctly. For a cooperative multi-hop networks over random error channels, the authors have proposed the use of MDS (Maximum Distance Separable) codes [8]. In the proposed scheme, the message to be forwarded is encoded at a relay node by an MDS code of coding rate $1/L$, where L is a positive integer. Then, a codeword is partitioned into L blocks and one of the L blocks is forwarded to neighboring nodes rather than the original message. At a receiving node, received codeword blocks are aggregated and then decoded with the MDS decoder. Assuming a simple tandem cooperative topology, the authors theoretically analyzed the performance of the proposed scheme in terms of the outage probability by means of a non-homogeneous absorbing Markov chain [8].

In this paper, we apply the protocol proposed in [8] to the flooding mechanism over a network with square-lattice topology and evaluate the delivery ratio by exhaustive computer simulations. It can happen that a relay node which failed in retrieving the message can receive other codeword blocks some other time. Therefore, in applying the protocol, we can suppose two decoding procedures of the MDS code employed at a relay node. One procedure is that a relay node discards received blocks if it fails to retrieve the message, whereas the other procedure is that a relay node stores the erroneous blocks in its memory for the sake of decoding invoked afterward.

The rest of the present paper is organized as follows: Section

Manuscript received December 10, 2012.

Shuji Kobayashi is with the Department of Information and Communication Engineering, Faculty of Computer Science and System Engineering, Okayama Prefectural University, Soja, 719-1197 Japan. (e-mail: s-koba@c.oka-pu.ac.jp).

Katsumi Sakakibara is with the Department of Information and Communication Engineering, Faculty of Computer Science and System Engineering, Okayama Prefectural University, Soja, 719-1197 Japan. (phone: +81-866-94-2109; Fax: +81-866-94-2199; e-mail: sakaki@c.oka-pu.ac.jp).

Jumpei Taketsugu is with the Department of Information and Communication Engineering, Faculty of Computer Science and System Engineering, Okayama Prefectural University, Soja, 719-1197 Japan. (e-mail: taketugu@c.oka-pu.ac.jp).

II briefly reviews useful properties of MDS codes and describes the outline of the protocol. Numerical results are presented in Section IV. Finally, Section V concludes the present paper.

II. SYSTEM MODEL

A. MDS Codes

Denote a linear block code of length n and dimension k over a certain finite field by an $[n,k]$ code. An $[n,k]$ code is MDS if its minimum distance is $n-k+1$. A class of MDS codes, including Reed-Solomon codes, is known to be fruitful in advantageous properties [9]. Among them, the following two theorems; Theorems 8-4 and 8-6 in [9], are used afterward:

Theorem 1 *For an $[n,k]$ MDS code, a receiver can recover the encoded message, if it receives at least k code symbols with no errors.* □

Theorem 2 *Punctured MDS codes are also MDS, that is, the minimum distance of an $[n-p,k]$ punctured MDS code is $n-p-k+1$, if $n-p \ge k$.* □

Suppose an $[Lk,k]$ MDS code, whose coding rate is $1/L$. Let $\boldsymbol{G}$ be a generator matrix of the $[Lk,k]$ MDS code. It is clear that $\boldsymbol{G}$ is a $k \times Lk$ matrix. Let

$$\boldsymbol{G} = [\ \underset{k}{\boldsymbol{G}_1}\ |\ \underset{k}{\boldsymbol{G}_2}\ | \cdots |\ \underset{k}{\boldsymbol{G}_L}\ ] \tag{1}$$

be the partition of $\boldsymbol{G}$ into L blocks of identical size, where $\boldsymbol{G}_\ell$ is a square matrix of order k for $\ell = 1,2,\cdots,L$. Similarly, a codeword of the $[Lk,k]$ MDS code can be also partitioned into L codeword blocks $\boldsymbol{c}_\ell$ of length k;

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G} = [\ \underset{k}{\boldsymbol{c}_1}\ |\ \underset{k}{\boldsymbol{c}_2}\ | \cdots |\ \underset{k}{\boldsymbol{c}_L}\ ] \tag{2}$$

where $\boldsymbol{m}$ is a message block of length k and $\boldsymbol{c}_\ell = \boldsymbol{m}\boldsymbol{G}_\ell$ for $\ell = 1,2,\cdots,L$. Then, from Theorem 1 and Theorem 2, the following corollary holds when a relay node receives one or more codeword blocks $\boldsymbol{c}_\ell$:

Corollary 1 *Assume that u distinct codeword blocks, $\boldsymbol{c}_{\ell_1}$, $\boldsymbol{c}_{\ell_2}$, $\cdots$, $\boldsymbol{c}_{\ell_u}$, are received $(u \le L)$ and that a receiver can identify the received codeword block number, ℓ_1, ℓ_2, $\cdots$, ℓ_u. Then, a k-symbol message $\boldsymbol{m}$ can be recovered, if either of the following conditions is satisfied:*

1) At least one codeword block $\boldsymbol{c}_\ell$ is error-free;

2) The total number of errors occurred in the u codeword blocks is less than or equal to

$$t_u = \left\lfloor \frac{(u-1)k}{2} \right\rfloor, \tag{3}$$

where $\lfloor x \rfloor$ is the maximum integer not greater than x. □

Proof: Since every codeword block $\boldsymbol{c}_\ell$ consists of k symbols, it apparently follows from Theorem 1 that a receiver can recover the message $\boldsymbol{m}$ from one or more error-free codeword blocks. This leads to the first condition.

Aggregation of the u distinct received codeword blocks results in a codeword of a $[uk,k]$ punctured MDS code. Thus, t_u or less errors can be corrected according to Theorem 2, which provides the second condition. (QED)

B. Network Model

We consider message broadcast in a network consisting of one source node and a number of relay nodes geographically dispersed on a two-dimensional plane. Here, a message to be broadcast consists of k symbols. We assume that no background traffic exists and that a channel between neighboring nodes occasionally adds symbol errors according to the independent and identically distributed random process with symbol error rate ε. It should be noticed here that, in order for a relay node to detect an error-free reception of a transmitted block, FCS (Frame Check Sequence) should be appended to every block.

The source node first broadcasts a message block $\boldsymbol{m}$ of k-symbol length to relay nodes within its transmission range. In conventional flooding without MDS codes [2][4], a relay node which can successfully obtain the message block $\boldsymbol{m}$ then forwards it to its neighboring relay nodes. This forwarding procedure continues. However, once a relay node has forwarded the message, it never re-broadcasts the same block even it receives the message again.

In contrast, in our protocol [8], a successful relay node encodes the message block $\boldsymbol{m}$ with an $[Lk,k]$ MDS code. One codeword block randomly selected among L blocks; $\boldsymbol{c}_1$, $\boldsymbol{c}_2, \cdots,$ $\boldsymbol{c}_L$, is then transferred to its next relay nodes. At a next relay node, an error-correcting procedure is invoked upon a reception of one or more blocks. Suppose that a relay node receives j blocks, where u distinct codeword blocks are included ($u = 1, 2, \cdots, j$). According to Corollary 1, the relay node attempts to retrieve the message block $\boldsymbol{m}$ among the j received codeword blocks. If the message block is successfully retrieved, then the relay node re-encodes the message block by the $[Lk,k]$ MDS code and broadcasts one randomly selected codeword block of length k among L codeword blocks. Notice here that if a relay node receives a block broadcast by the source node, then the message block can be recovered only when no symbol errors are included similarly to the conventional flooding. Also, for simplicity, we assume that a relay node can receive two or more blocks simultaneously.

Example 1 Let us suppose that a relay node receives 5 codeword blocks, more precisely, 4 $\boldsymbol{c}_1$'s and 1 $\boldsymbol{c}_2$, as shown in Fig. 1. In this case, we have $j=5$ and $u=2$. To this end, Corollary 1 guarantees that the relay node can recover the message block $\boldsymbol{m}$, if at least one error-free codeword block exists among the $j=5$ received ones or if the number of symbol errors in the aggregated block of $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$; $[\ \boldsymbol{c}_1\ |\ \boldsymbol{c}_2\ ]$, is at most $t_2 = \lfloor k/2 \rfloor$, even when all the 5

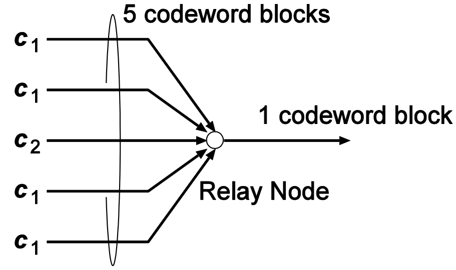
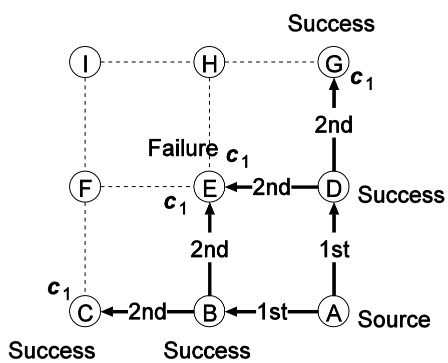
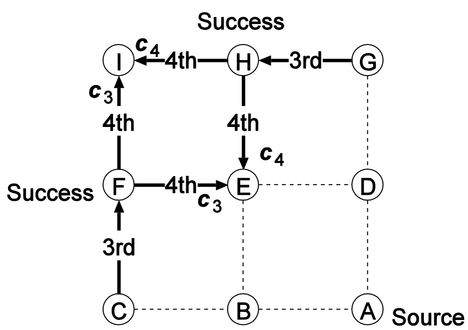


Fig. 1. A relay node receives $j = 5$ codeword blocks, but $u = 2$ distinct ones, $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$, are included.



(a) 1st and 2nd hops



(b) 3rd and 4th hops

Fig. 2. Illustrative example of codeword block relaying in a lattice-pattern network of nine nodes for $L = 4$. A dashed line connects nodes within transmission range and a solid line is block transmission, where a numeral on solid line represents the hop number.

received codeword blocks include one or more symbol errors. □

III. Two Decoding Procedures at Relay Node

Since it is assumed that a relay node is able to simultaneously receive two or more blocks, we can suppose two type of decoding procedures at a relay node according to the availability of memory for received blocks. If no memory is equipped at a relay node, received blocks are discarded when the node failed in retrieving the message block. On the contrary, if a relay node can store the received blocks, the decoding procedure can be carried out by aggregating currently received blocks with stored blocks. The latter might enhance the error-correcting capability of the MDS codes, compared to the former. The following example illustrates the procedures.

Example 2 Let us consider a broadcast network of nine nodes, where nodes are located in a square-lattice pattern, as shown in Fig. 2. Neighboring nodes, that is, nodes within the transmission range of each other are connected by dashed lines, and block transmissions are drawn by solid lines with the hop number. Here, it is assumed that $L = 4$.

Node A is the source node. At the first hop, Node A broadcasts the message block $\boldsymbol{m}$ to Nodes B and D and both nodes receive $\boldsymbol{m}$ with no errors. Each of Nodes B and D encodes the message block $\boldsymbol{m}$ by a $[4k, k]$ MDS code. At the second hop, codeword block $\boldsymbol{c}_1$ is randomly selected by Node B and so is occasionally by Node D. Node E receives two identical codeword blocks; $\boldsymbol{c}_1$, and both are received with errors. Hence, Node E failed in recovering the message block $\boldsymbol{m}$, as indicated in Fig. 2(a), since no error correction ban be available. Here, if a relay node possesses memory devices, Node E stores the two erroneously received codeword blocks $\boldsymbol{c}_1$. Then, codeword block transmissions continue, as shown in Fig. 2(b). At the fourth hop, Node E receives two codeword blocks; $\boldsymbol{c}_3$ from Node F and $\boldsymbol{c}_4$ from Node H. If both $\boldsymbol{c}_3$ and $\boldsymbol{c}_4$ are impaired by symbol errors and if the two previously received $\boldsymbol{c}_1$ are stored at Node E, then three received codeword blocks, $\boldsymbol{c}_1$, $\boldsymbol{c}_3$ and $\boldsymbol{c}_4$, can be aggregated, so that the decoding procedure of a $[3k, k]$ MDS code is invoked. On the other hand, if no memory is equipped at a relay node, the decoding procedure of a $[2k, k]$ MDS code is carried out for $[\ \boldsymbol{c}_3 \mid \boldsymbol{c}_4\ ]$. In the latter case without memory, the probability of successful recovery of $\boldsymbol{m}$ is clearly less than that in the former case, since the error correcting capability is $t_3 = k$ and $t_2 = \lfloor k/2 \rfloor$ for the case with memory and the case without memory, respectively. □

IV. Numerical Example

We examine the performance of the proposed procedure by means of exhaustive computer simulations. Three cases for the use of MDS codes are supposed; $L = 2,3,4$, for the message length $k = 64$, so that a $[128, 64]$ MDS code, a $[192, 64]$ MDS code, and a $[256, 64]$ MDS code are employed for $L = 2,3,4$, respectively. The symbol error rate is set to $\varepsilon = 10^{-2}$.

As a simple example, we consider a network consisting of 121 nodes, which are located in a square-lattice pattern [5][10]–[12], as shown in Fig. 3. In Fig. 3, the source node, which is placed at the center, is denoted by the black circle and relay nodes are denoted by a circle. Solid lines represent random

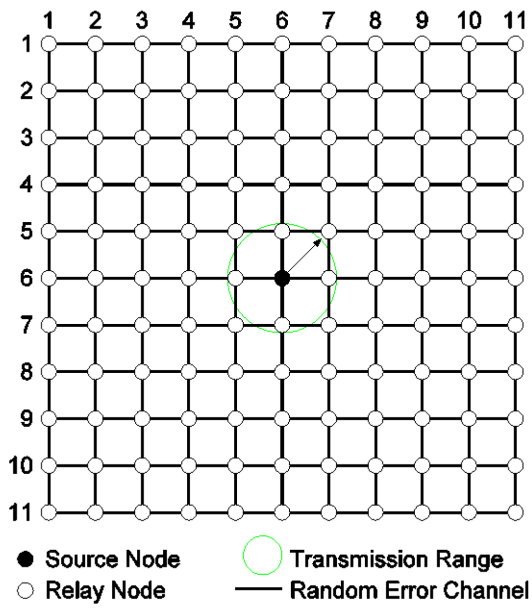
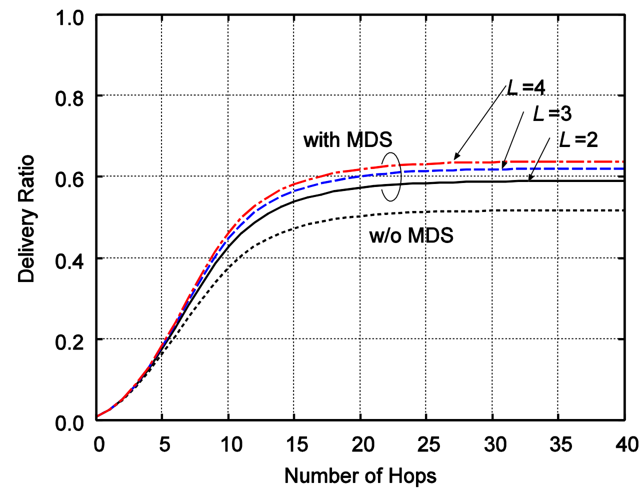


Fig. 3. Network consisting of 121 nodes in square-lattice topology.

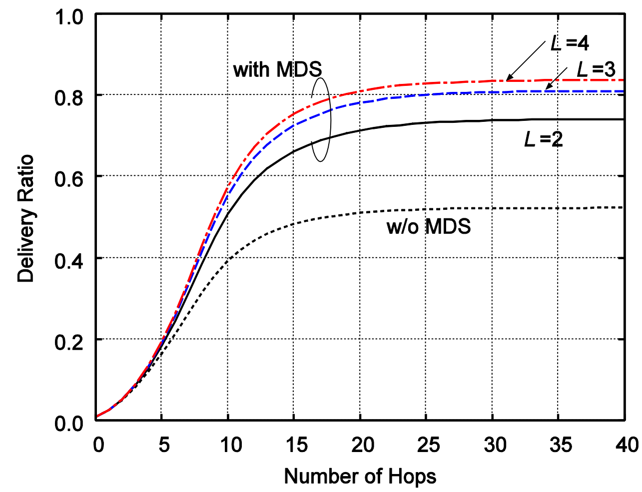
error channels between neighboring nodes. The ratio of nodes which successfully recover the message block $\boldsymbol{m}$ is given in Fig. 4 as a function of the hop number. In Fig. 4(a), the results for the case where no memory can be available at a relay node are provided and Fig. 4(b) shows the results for the case of relay nodes with memory. The results are obtained by averaging 1,000 trials. It is apparent that the initial delivery ratio is 1/121, since the source node is the only one which has the message and no other nodes possess it.

In Fig. 4, every curve is saturated after approximately 20 hops. It implies that no more relay nodes can retrieve the message block and no further broadcast can be expected in this case. From Fig. 4 it can be observed that only 50% of nodes can obtain the message block $\boldsymbol{m}$, if no MDS codes are employed in spite of the availability of memory at a relay node. It is no use to store erroneously received blocks at a relay node if no MDS codes are employed, since no error correcting capability is available. The use of a MDS code can improve the delivery ratio. Particularly, the delivery ratio can be increased more when a longer MDS code is employed in conjunction with memory at a relay node. For example, more than 60% improvement can be achieved for $L=4$, as shown in Fig. 4(b). This improvement can be obtained even for small L if a relay node can store the previously received codeword blocks and can make use of them by aggregation in the decoding procedure, as shown in Example 2. In square-lattice topology, a node connects to four adjacent nodes except for a node located at the edge of the network. Hence, it can be possible for a relay node to correct symbol errors by means of the $[4k, k]$ MDS code for $L \geq 4$ when it occasionally happen that the four adjacent nodes select different codeword blocks.

Next, Fig. 5 presents the distribution of u, the number of



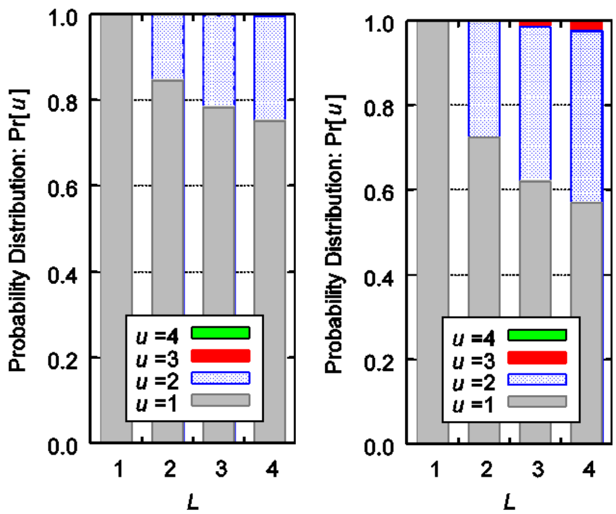
(a) without memory at a relay node



(b) with memory at a relay node

Fig. 4. The ratio of nodes which successfully recover the message block $\boldsymbol{m}$ of length $k=64$ for $\varepsilon=10^{-2}$ and for 121 nodes located in a square-lattice pattern, as shown in Fig. 3.

different codeword blocks which can be aggregated in the decoding procedure. Clearly, it holds that $\Pr[u=1]=1$ and $\Pr[u>1]=0$ for the case without MDS codes; $L=1$. Similarly to Fig. 4, Fig. 5(a) provides the case where no memory can be available at a relay node and Fig. 5(b) is the results for the case of relay nodes with memory. The probability of $u \geq 3$ is less than 1% when no memory is available at a relay node and it is approximately 1.5% for $L=3$ with memory and 2.6% for $L=4$ with memory. Comparing two graphs in Fig. 5 for identical L, we can recognize that increment of the probability of $u=2$ improves the delivery ratio for the case of a relay node with memory. For $k=64$ and $\varepsilon=10^{-2}$, the probability of erroneous reception of a single block is $1-(1-\varepsilon)^k \approx 0.47$. However, when two different codeword blocks are aggregated, the probability of decoding failure for a [128, 64] MDS code is



(a) without memory at a relay node (b) with memory at a relay node

Fig. 5. The distribution of the number of aggregated codeword blocks of length $k = 64$ when the decoding procedure is carried out for $\varepsilon = 10^{-2}$ and for 121 nodes located in a square-lattice pattern, as shown in Fig. 3

$$\sum_{i=33}^{128} \binom{128}{i} \varepsilon^i (1-\varepsilon)^{128-i} \approx 1.7 \times 10^{-37} \tag{4}$$

since $t_2 = 32$ symbol errors or less can be corrected from the second condition in Corollary 1. This value is negligibly small. Hence, in most cases, a relay node can recover the message block $\boldsymbol{m}$ if it receives two different codeword blocks.

V. Conclusion

We have applied the random relaying of codeword blocks of an MDS code [8] to the flooding over random error channels. A message block to be broadcast is encoded by an MDS code of coding rate $1/L$, where L is an integer. A relay node partitions a codeword of the MDS code into L blocks and transmits one randomly selected codeword block. When each relay node receives two or more codeword blocks of the MDS code, it aggregates the blocks, corrects channel errors with the aid of the MDS code or its punctured code. The delivery ratio of the broadcast message in a network with square-lattice topology has been evaluated by means of computer simulation. In applying the protocol, we have supposed two decoding procedures of the MDS code employed at a relay node according to the availability of memory to store erroneously received blocks. One procedure is that a relay node discards received blocks if it fails to retrieve the message, whereas the other procedure is that a relay node stores the erroneous blocks in its memory for the sake of decoding invoked afterward.

Numerical results for a network with 121 nodes reveal that significant improvement can be achieved, in particular, for a long MDS code and for relay nodes with memory. This performance improvement stems from powerful error-correcting capability of an MDS code.

Further studies include, for instance, application of the proposed protocol to networks of other topology and consideration of the backoff algorithm in the MAC sub-layer.

References

[1] C.-K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and systems*, Prentice-Hall, Englewood Cliffs, NJ, 2002.

[2] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proc. ACM MobiCom '99*, Seattle, WA, pp. 151–162, Aug. 1999.

[3] P. Mannersalo, A. Keshavarz-Haddad and R. Riedi, "Broadcast flooding revisited: Survivability and latency," in *Proc. IEEE INFOCOM 2007*, Anchorage, AK, pp. 652–660, May 2007.

[4] G. Vakulya and G. Simon, "Energy efficient percolation-driven flood routing for large-scale sensor networks," in *Proc. Intl. Multiconf. Comput. Sci. & Inform. Tech. (IMCSIT 2008)*, Wisla, Poland, pp. 877–883, Oct. 2008.

[5] V. Raman and I. Gupta, "Performance tradeoffs among percolation-based broadcast protocols in wireless sensor networks," in *Proc. Intl. Conf. Distributed Computing Syst. (ICDCS 2009)*, Montreal, Canada, pp. 158–165, June 2009.

[6] M.-K. Chang, C.-A. Shen and M.-H. Chuang, "New results on the connectivity in wireless ad hoc networks," in *Proc. IEEE Veh. Tech. Conf. (VTC-Spring 2012)*, Yokohama, Japan, June 2012.

[7] Y. Oishi, H. Murata, K. Yamamoto and S. Yoshida, "Theoretical FER performance of multi-hop wireless cooperative networks using transit diversity," in *Proc. IEEE Veh. Tech. Conf. (VTC 2008-Spring)*, Singapore, Singapore, pp. 2366–2369, May 2008.

[8] K. Sakakibara, D. Ito and J. Taketsugu, "Outage probability of random relaying of MDS codeword blocks in cooperative multi-hop networks," in *Proc. Intl. Conf. Inform. Networking (ICOIN 2011)*, Kuala Lumpur, Malaysia, Jan. 2011.

[9] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, Englewood Cliffs, NJ, 1995.

[10] Z. Ren, Z. Deng, Z. Sun and D. Shuai, "Behaviours of networks with different topologies and protocols," *Computer Physics Commun.*, vol. 141, no. 2, pp. 247–259, Nov. 2001.

[11] D. K. Arrowsmith, R. J. Mondragon and M. Woolf, "Data traffic, topology and congestion," in L. Kocarev and G. Vattay (Eds.) *Complex Dynamics in Communication Networks*, Springer, Heidelberg, Germany, 2005.

[12] H. Kawahigashi, T. Terashima, N. Miyauchi and T. Nakakawaji, "Modeling ad hoc sensor networks using random graph theory," in *Proc. IEEE Consumer Commun. & Networking Conf. (CCNC 2005)*, Las Vegas, NV, pp. 104–109, Jan. 2005.