Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 8 (18): 3273-3278, 2008
ISSN 1812-5654

Improving Fault Tolerance in Ad-Hoc Networks by Using Residue Number System

[1]A. Barati, [2]M. Dehghan, [3]A. Movaghar and [1]H. Barati
[1]Islamic Azad University, Dezful Branch, Dezful, Iran
[2]Amirkabir University of Technology, Tehran, Iran
[3]Sharif University of Technology, Tehran, Iran

Abstract: In this study, we presented a method for distributing data storage by using residue number system for mobile systems and wireless networks based on peer to peer paradigm. Generally, redundant residue number system is capable in error detection and correction. In proposed method, we made a new system by mixing Redundant Residue Number System (RRNS), Multi Level Residue Number System (ML RNS) and Multiple Valued Logic (MVL RNS) which was perfect for parallel, carry free, high speed arithmetic and the system supports secure data communication. In addition it had ability of error detection and correction. In comparison to other number systems, it had many improvements in data security, error detection and correction, speed of storage and retrieval.

Key words: Wireless networks, RNS, error detection and correction, fault tolerant system, coding theory

INTRODUCTION

Mobile ad-hoc network (MANET) is an efficient technology for providing a wide-area communication environment where installing the infrastructure of a wired network is difficult. It is also suitable for supporting communication among mobile nodes. For the last several decades, many routing protocols have been proposed to make the best use of wireless network technology (Abolhasan *et al*., 2004; Xiaoyan *et al*., 2002; Royer and Toh, 1999; Barati *et al*., 2007a).

As making base station or wired networks for mobile terminal is impossible or unfeasible use of these networks owing to simple configuration and low cost is very suitable. Some applications are communication in hostile environment without any central base station, navies in navy component, mobile computer meetings of people in areas where wired networks are not available, disaster recovery, management of emergencies (for instance in case of earth quake where all infrastructures are destroyed).

The major issue in ad-hoc networks is how to implement dependable and secure data storage. This is an essential requirement in applications where the mobiles cooperate by sharing information and need to create and access shared files. In this situation the system should prevent data losses or corruption due to network disconnections, mobile failures or malicious attacks from untrustworthy mobiles (Satyanarayanan *et al*., 1990).

On the other hand ad-hoc networks are a heterogeneous mix of different wireless and mobile devices, ranging from little hand-held devices to laptops. Such devices are dependable on batteries for energy consumption, in case of battery depletion which is similar to a crash fault; the mobile may not recover data upon the availability of battery replacement/recharge. As mobiles may not be equipped with permanent storage, failures may result in data losses or corruption. For all of these reasons, many techniques are presented for solving dependable and secure data storage problem up to now, one of these techniques is using residue number system.

The Residue Number System (RNS) is an unconventional and non weighted number system, which is capable of supporting parallel, carry free, high speed arithmetic. In this system, arithmetic operations act on residues-reminder of dividing original number in several definite moduli-in parallel. Consequently computations on these residues which are smaller than the original number are performed, so speed up arithmetic and decreased power consumption is achieved (Szabo and Tanaka, 1967).

A residue number system is characterized by a moduli set $\{m_1,m_2,...,m_n\}$ where the moduli, $m_i (i = 1,2,...,n)$ are pair-wise relatively prime (Parhami, 2001). Any integer X in the dynamic range, $M = m_1,m_2,...,m_n$, is represented by an N-tuple $(x_1,x_2,x_3,...,x_n)$, where x_i is the residue of X in moduli m_i for $i = 1,2,...,n$.

The reconstruction of X from its residue $(x_1,x_2,x_3,...,x_n)$ is based on the Chinese Reminder Theory (CRT) shown by:

Corresponding Author: Ali Barati, Department of Computer, Islamic Azad University, P.O. Box 313, Dezful Branch, Dezful, Iran
Tel: +98 641 6262090 Fax: +98 641 6262090

$$X = \left\langle \sum_{i=1}^{n} (x_i N_i)_{m_i} \times M_i \right\rangle_M$$

$$M = \prod_{i=1}^{n} M_i$$

$$M_i = \frac{M}{m_i},\ N_i = \left\langle M_i^{-1} \right\rangle_{m_i},\ i = 1, 2, 3, \ldots, n \quad (1)$$

The notation $\langle M_i^{-1} \rangle_{mi}$ in (1) denotes the multiplicative inverse of M_i moduli m_i.

Another advantage of this is security because for RNS conversion to weighted number system knowledge of moduli is required. Consequently this system is a symmetric key encryption system with medium security.

Some applications of RNS are digital signal processing, digital filters (Conway and Nelson, 2004), coding theory (How *et al*., 2006), RSA encoding algorithm (Bajard and Imbert, 2004), digital communication, ad-hoc networks, distributed dependable and secure data storage and retrieval (Barati and Movaghar, 2007b), error detection and correction (Barsi and Maestrini, 1973; Krishna *et al*., 1992; Sun and Krishna, 1992) and fault tolerant system.

In addition, in this system owing to separate computation on residues if error occurs one of this residues, the effect of it is not distributed on other residues. In other words RNS architectures inherently are fault tolerant (Kinoshita and Lee, 1997).

MULTI LEVEL RESIDUE NUMBER SYSTEM (ML RNS)

Arithmetic computations on each moduli could be done with a new residue number system and repeated until having very small moduli owing to residue number systems properties in increasing calculations speed, decreasing power consumption, increasing security and fault tolerance. In other words this process could be repeated for several levels.

The system derived from the process is called Multi Level Residue Number System (MLRNS). However in this system the dynamic range of any sub-residue number system like residues in ith level must be grater than the largest moduli in the previous level like residues in (i-1)th level. In this paper two level residue number system is assumed in order to simplify the presentation. It should be considered that provided method could be expanded for more levels as well (Yassine, 1992).

In residue number system with two levels, two symmetrical key encryption algorithms are used in together, so the system has a high security. Another advantage of two levels residue number system is the simple selection moduli set for large presentation limits. This means by selecting a few large modulis and using a new residue system with smaller moduli for second level accordingly this capability is achieved. By having a few numbers of great moduli in first level as a result; First the problem of being pair-wise relatively prime of moduli also unbalancing of them would be solved and second, owing to use of less moduli the converting circuits are simple the conversions would be done rapidly. Meanwhile since modulis in second level are small, internal computations of residue number system-because of short carry propagation are performed rapidly (Skavantzos and Abdallah, 1999).

Notations that used for two residue number system in this paper are as following:

$\{m_1, m_2, m_3, \ldots m_n\}$	:	First level residue number system moduli set
$\{m_{i1}, m_{i2}, m_{i3}, \ldots m_{in_i}\}$	:	Second level residue number system moduli set for moduli m_i(i = 1,2,3,...,n)
$(r_1, r_2, r_3, \ldots, r_n)$	:	Residues in first level residue number system
$(r_{i1}, r_{i2}, r_{i3}, \ldots, r_{in_i})$	:	Residues in second level for r_i(i = 1,2,3,...,n)

Arithmetic computations in two level residue number system are performed on the second level residues. Two operand arithmetic operations are defined as following:

$$\{z_{i1}, z_{i2}, z_{i3}, \ldots, z_{in_i}\} = \{x_{i1}, x_{i2}, x_{i3}, \ldots, x_{in_i}\} \circ \{y_{i1}, y_{i2}, y_{i3}, \ldots, y_{in_i}\} \quad (2)$$

where, $z_{ij} = (x_{ij} o y_{ij}) \bmod m_{ij}$, i = 1,2,3,...n, j = 1,2,3,...n and o could be addition, subtraction and multiplication (Hosseinzadeh and Navi, 2007).

For conversion from weighted number system to two level residue number system first of all the supposed number should be converted to first level residue number system and the supposed residues should be converted to second level residue number system. This process is shown in Fig. 1.

In reverse conversion, $n \times n_i$-channel CRT for i = 1,2,3,...,n it is necessary to convert second level residues to equal residues in first level and then convert to weight number system by using a n_i-channel CRT. This process is shown in Fig. 2.

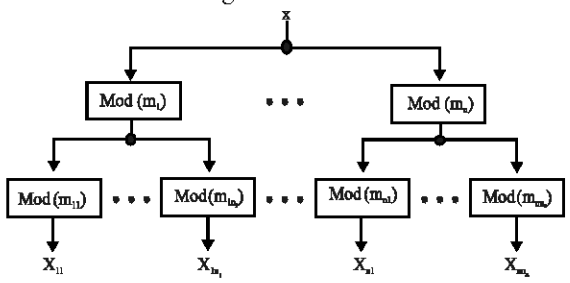

Fig. 1: Conversion from weighted number system to two level residue number system

MULTIPLE VALUED LOGIC (MVL RNS)

Multi-valued logics are logical calculi in which there are more than two truth values. Traditionally, logical calculi are two-valued, that is, there are only two possible truth values (i.e., truth and falsehood) for any proposition to take. An obvious extension to classical two-valued logic is an n>2-ary logic. Those most popular in the literature are three-valued and infinite-valued ones.

It is obvious that the positional weights of any two succeeding columns are multiples of r. Figure 3 represents the positional value of each location.

Each location in an MVL component can store much more information than a binary logic component, the dynamic range of the moduli set $\{r^n-2, r^n-1, r^n\}$ is much greater than its equivalent in the binary representation. Now the question is how to present the related hardware which is clearly answered in (Skavantzos and Abdallah, 1999) (r = 10 in this research).

REDUNDANT RESIDUE NUMBER SYSTEM

Additional moduli is used in residue number system for error detection and correction capability. This system is called Redundant Residue Number System (RRNS). Redundant residue number system is presented by:

$$\{m_1, m_2, \ldots, m_{h,m_{h+1}}, \ldots, m_{h+r}\} \text{ and } m_i > m_{i-1} \quad (3)$$

In case all moduli were pair-wise relatively prime the presentation limit of this system is equal to:

$$\left[0, \prod_{i=1}^{h+r} m_i\right] \quad (4)$$

The interval [0,M] that $M = \prod_{i=1}^{h} m_i$ constitutes the legitimate range and the interval [M, M×M_R] that $M_R = \prod_{i=h+1}^{h+r} m_i$ is associated so-called illegitimate range. Any

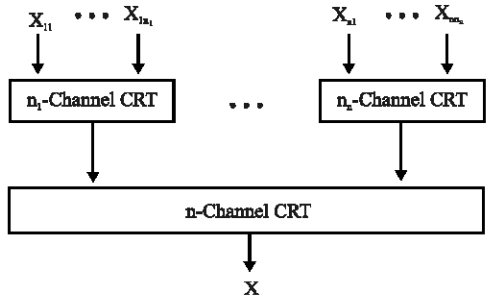

Fig. 2: Conversion from two level residue number system to weight number system

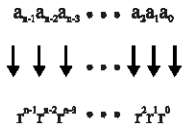

Fig. 3: Positional weight value of each location

integer belonging to the legitimate range will be labeled as legitimate and those belonging to the illegitimate range as illegitimate.

In redundant residue number system with h+r moduli, a number like X that $\alpha \le X < \alpha+M$ is represented by $(x_1, x_2, \ldots, x_h, x_{h+1}, \ldots, x_{h+r})$.

The minimum distance d_{min} is a fundamental parameter associated with any error control code. The minimum distance of an RRNS code is d_{min} if and only if the product of redundant moduli satisfies the following relation:

$$\max\{\prod_{i=1}^{d-1} m_{j_i}\} \le M_R < \max\{\prod_{i=1}^{d} m_{j_i}\}, 1 \le j_i \le h+r \quad (5)$$

As a result the minimum hamming distance of a redundant number system is 3, if and only if:

$$\max\{m_{j_1}, m_{j_2}\} \le M_R < \max\{m_{j_1}, m_{j_2}, m_{j_3}\} \quad 1 \le j_1, j_2, j_3 \le h+r \quad (6)$$

For example if a supposed redundant residue number system with moduli set of $(m_1, m_2, m_3, m_4, m_5, m_6)$ = (3,7,11,13,16,17) for d = 3 should $272 \le M_R < 3536$.

So minimum distance of 3 will be derived from each of these sets:

$$\{m_5, m_6 : M_R = 272\}$$
$$\{m_1, m_2, m_4 : M_R = 273\}$$
$$\{m_1, m_2, m_5 : M_R = 336\} \quad (7)$$

In addition if we choose moduli $\{m_1, m_2, m_3, m_4, m_5: M_R = 3696\}$ minimum distance of 4 will be derived.

As we see choosing redundant moduli set for minimum Hemming distance is non-unique. For choosing the optimal redundant moduli set in order to maximize the amount of M according to equation M×M_R = C in which C is a constant number, M_R should be minimized. The least M_R for minimum Hemming distance is equal to:

$$M_R = \max\{\prod_{i=1}^{d-1} m_{j_i}\} \quad ,1 \le j_i \le h+r \quad (8)$$

In optimal redundant number system d−1 big moduli of it should be chosen for minimum Hemming distance. In other words:

$$d-1=(h+r)-h \Rightarrow d=(h+r)-h+1=r+1 \quad (9)$$

Consequently in optimal redundant number system the minimum Hemming distance is equal to r+1 (Barsi and Maestrini, 1973). From here optimal redundant number system is meant by redundant number system.

In redundant residue number system if h residues were achieved among h+r residues then we could recovered the number X. This property makes error detection and correction possible in redundant residue number system which is the basis of error detection and correction as well.

$$\left(\prod_{i=1}^{h} m_{j_i}=M' \quad ,1\le j_i\le n\right)\Rightarrow M<M' \Rightarrow \alpha\le X<M<M'\Rightarrow \alpha\le X<M' \quad (10)$$

Derivation of X from h option moduli is possible according to these equations by using Chinese Reminder Theory.

Coding properties of redundant residue number system is similar to RS famous codes. As a result by considering the minimum Hemming distance of this code is r+1:

This code has the capability of detection r corrupted residues.

- This code has the capability of correcting $\lfloor r/2 \rfloor$ corrupted residues.
- This code has the capability of simultaneous correcting up to λ corrupted residues and detection up to β corrupted residues ($\beta>\lambda$), if and only if $\lambda+\beta\le r$.
- This code has the capability of simultaneous detection of t errors and detection of s residues which are corrupted in the path and hasn't arrived, if and only if $t+s\le r$.

This code has the capability of simultaneous correction of t errors and correction of s residues which are corrupted in the path and hasn't arrived, if and only if $2t+s\le r$.

MVL ML REDUNDANT RESIDUE NUMBER SYSTEM AND ITS APPLICATION IN AD-HOC NETWORKS

MVL ML redundant residue number system: In this article multi level redundant residue number system is presented for increasing error detection and correction and increasing security in high speed computing without carry propagation. In multi level redundant residue number system, redundant moduli could be used for error detection and correction. Many errors could be detected or corrected in low levels in this method.

Multi level redundant residue number system has the capability to provide much fault tolerance for more important moduli in first level, in this method moduli which are supposed for lower levels of redundant residue number system have more redundancy or have more Hemming distance in other words. There is an important issue in this system. The error detection and correction of RRNS coding are performed on moduli not on bits (Note a moduli might be single bit or more). Therefore if a single-bit-error has occurred, the whole moduli will be involved. So, the rate of error detection and correction will be increase for single-bit-error by using small moduli.

Application of MVL ML redundant residue number system in ad-hoc network units: The data storage and retrieval in Ad-Hoc network provides by cooperating the mobiles in creating and sharing files and the system provides procedures for the users to create, share, read and delete the files. For each mobile in ad-hoc network is defined $U_i(i = 1,2,...)$ that is unique in the network. In the rest of the section we describe the file creation, sharing, reading and removal procedures.

- **File creating:** Two-level redundant residue number system is used for creating encoded a file. For this purpose a two-Level moduli set realized with described specifications. This moduli set could be selected in offline situation as well the number system presentation limit should just be selected greater than the proposed file.

  In case of files with huge volume, partitioning into small sub-file could be used. Each file coded $\sum_{i=1}^{n} h_i + r_i$ to residue and each residue is sent to different mobiles. The selected mobile stores the received residue in its storage. The assignment of mobiles to residues is arbitrary with the only constraint that different residues of the same record should be stored in different mobiles, while residues shouldn't include any information about the moduli which they are encoded with.

  The file owner have a description file that containing moduli set used for encoding any file along with description about mobiles storing residue. This file is hidden and kept by the owner.

- **File reading:** For reconstruct the file each residue and its corresponding moduli which is coded with it is required because of this coding property.

If U_t has a copy of description file, it could order different part of file from other mobiles according to the description file. So U_t could reconstruct the file upon receiving sufficient $\sum_{i=1}^{n} h_i$ residues by using Chinese Remainder Theorem.

But during reading execution some of inquiries might be lost or corrupted in the network before reaching U_t. In such situation detection and or correction might be able depending on the amount of received additional residue.

- **File sharing:** The file owner could share the file for trustworthy mobiles upon request by sharing the description file. The file owner could even define access level to this file for other mobiles. For example access only for reading, writing, reading and writing.

- **File removal:** File deletion could only be done by owner while the owner could grant this right to others. File deletion is performed upon sending a message for mobiles having residue.

COMPARISON

A comparison between redundant residue number system (Bajard and Imbert, 2004) and MVL ML redundant residue number system for secure and reliable data storage and retrieve is shown in Table 1.

Error detection and correction is increased in multi-level redundant residue number system owing to moduli Detection and correction capability (because each moduli itself is constructed by a residue number system). Security achieved by using multi-level redundant residue number system is much higher than redundant residue number system by using multiple of symmetric encryption code together.

In multi-level redundant residue number system, residues are less significant amounts because of using small moduli and could be transmitted rapidly and computations on these residues is also very fast. Achieved presentation range is very large by using multi-level redundant residue number system and that is no problem in moduli selection and these would be no limits for file size consequently.

Table 1: MVL ML redundant residue number system comparison with redundant residue number system

Parameters	MVL ML RRNS	MVL MLRNS	ML RNS	RRNS	RNS
Error correction	High	No	No	Normal	No
Error detection	High	No	No	Normal	No
Security	High	Normal	High	Normal	Minimum
Speed in send	High	Normal	High	Normal	Normal
Speed in computing	High	Normal	High	Normal	Normal
Size of file limitation	Very Large	Very Large	Large	Large	Normal

CONCLUSION

In this research, multi-level residue number system, multiple Valued Logic and redundant residue number system are surveyed and then MVL ML redundant residue number system and application of this number system in ad-hoc networks was presented accordingly.

MVL ML redundant residue number system has more security, error detection and correction capability and more speed in comparison to activities done before in this case.

Since the amount of minimum Hamming Distance in multi-level redundant residue number system, is equal to $\sum_{i=1}^{n}(r_i+1)$ So:

If in each second level moduli which is assumed for first level of ith moduli (i = 1,2,...,n), up to maximum r_i error occur, then the system can detect $\sum_{i=1}^{n} r_i$ error.

If in each second level moduli which is assumed for first level of ith moduli (i = 1,2,...,n), up to maximum $\lfloor r_i/2 \rfloor$ error occur, then the system can correct $\sum_{i=1}^{n}\left\lfloor \frac{r_i}{2} \right\rfloor$ error.

If in each second level moduli which is assumed for first level of ith moduli (i = 1,2,...,n), up to maximum $\lambda_i + \beta_i \le r_i$ that $\lambda_i < \beta_i$ residues are corrupted, then this code capable of correcting λ errors and simultaneously detecting β errors, if and only if

$$\beta = \sum_{i=0}^{n} \beta_i \text{ and } \lambda = \sum_{i=0}^{n} \lambda_i$$

If in each second level moduli which is assumed for first level of ith moduli (i = 1,2,...,n), up to maximum t_i error occur and also s_i residue never reached, then this code capable of detecting t errors and simultaneously correcting s errors, if and only if

$$t_i + s_i \le r_i \quad \left(t = \sum_{i=0}^{n} t_i \text{ and } s = \sum_{i=0}^{n} s_i \right)$$

If in each second level moduli which is assumed for first level of ith moduli (i = 1,2,...,n), up to maximum t_i error occur and also s_i residue never reached, then this code capable of detecting t errors and simultaneously correcting s errors, if and only if

$$2t_i + s_i \le r_i \quad \left(t = \sum_{i=0}^{n} t_i \text{ and } s = \sum_{i=0}^{n} s_i \right)$$

ACKNOWLEDGMENT

We are grateful to Islamic Azad University of Dezful for financial support.

REFERENCES

Abolhasan, M., T. Wysocki and E.A. Dutkiewicz, 2004. A review of routing protocols for mobile Ad Hoc. Networks, 2: 1-22.

Bajard, J.C. and L. Imbert, 2004. Brief contributions: A full RNS implementation of RSA. IEEE Trans. Comput., 53: 769-774.

Barati, A. and A. Movaghar, 2007a. Dependable and secure data storage and retrieval in Ad-Hoc networks. Proceedings of the 1st International Conference on Digital Communications and Computer Applications (DCCA, 2007). March 19-22, Ibrid, Jordan, pp: 1299-1305.

Barati, A., A. Movaghar, M.R. Eslami Nejad and A. Bazrgar, 2007b. Presenting an on-demand routing algorithm for wireless mobile Ad-Hoc networks. Proceedings of 12th Annual International CSI Computer Conference. January 2007, Tehran, Iran, pp: 656663-663 (In Persian).

Barsi, F. and P. Maestrini, 1973. Error correcting properties of redundant residue number systems. IEEE Trans. Comput., C-22: 307-315.

Conway, R. and J. Nelson, 2004. Improved RNS FIR filter architectures. IEEE Trans. Circuits Syst. II: Express Briefs, 51: 26-28.

Hosseinzadeh, M. and K. Navi, 2007. A new moduli set for residue number system in ternary valued logic. J. Applied Sci., 7: 3729-3735.

How, H.T., T.H. Liew, E.L. Kuan, L.L. Yang and L. Hanzo, 2006. A redundant residue number system coded burst-by-burst adaptive joint-detection based CDMA speech transceiver. IEEE Trans. Vehicular Technol., 55: 387-396.

Kinoshita, E. and K. Lee, 1997. A residue arithmetic extension for reliable scientific computation. IEEE Trans. Comput., 46: 129-138.

Krishna, H., K.Y. Lin and J.D. Sun, 1992. A coding theory approach to error control in redundant residue number systems-Part I: Theory and single error correction. IEEE Trans. Circuits Syst. II: Analog Digital Signal Proc., 39: 8-17.

Parhami, B., 2001. Computer Arithmetic: Algorithms and Hardware Designs. 1st Edn., Oxford University Press, Oxford, UK., ISBN: 0-19-512583-5 .

Royer, E.M. and C.K. Toh, 1999. A review of current routing protocols for Ad-Hoc mobile wireless networks. IEEE Pers. Commun., 6: 46-55.

Satyanarayanan, M., Kistler, J.J. Kumar, P. Okasaki, M.E. Siegel and E.H. Steere, 1990. Coda: A highly available file system for a distributed workstation environment. IEEE Trans. Comput., 39: 447-459.

Skavantzos, A. and M. Abdallah, 1999. Implementation issues of the two-level residue number system with pairs of conjugate moduli. IEEE Trans. Signal Proc., 47: 826-838.

Sun, J.D. and H. Krishna, 1992. A coding theory approach to error control in redundant residue number systems -Part II: Multiple error detection and correction. IEEE Trans. Circuits Syst. II: Analog Digital Signal Proc., 39: 18-34.

Szabo, N.S. and R.I. Tanaka, 1967. Residue Arithmetic and Its Applications to Computer Technology. 1st Edn., McGraw-Hill, New York, ISBN:0-8186-0811-0 .

Xiaoyan, H., X. Kaixin and M. Gerla, 2002. Scalable routing protocols for mobile ad hoc networks. IEEE Network, 16: 11-21.

Yassine, H.M., 1992. Hierachical residue number system suitable for VLSI arithmetic architectures. IEEE Int. Sympo. Circuits Syst., 2: 811-814.