

The background is a dark, textured black with a grid of small dots. Overlaid on this are several thick, curved lines in various colors: a prominent blue line, a yellow line, a red line, and a green line. There are also dashed lines in these colors. In the bottom-left corner, there are several overlapping circles in shades of orange, red, and purple. The text is centered and rendered in a bold, yellow, serif font.

WCN 2010

15 October, Berlin, Germany

**Improved Data Communication in
WSN Using Modular Arithmetic**

Vasyl Yatskiv, Anatoly Sachenko, Natalia Yatskiv

Research Institute for Intelligent Computer
Systems, Ternopil National Economic University
and Glushkov Institute of Cybernetics, Ukraine

Outline

- **Introduction**
- **Existing Methods to Improve the Data Transmission Reliability**
- **Proposed Method of Multipath Routing**
 - **Coding Based on Residue Number System**
 - **Multipath Routing Algorithm**
- **Comparative Estimation of Sharing Methods and Experimental Results**
 - **Shamir's Threshold Scheme for Secret Sharing**
 - **Asmuth-Bloom's Threshold Scheme for Secret Sharing**
 - **The Coding Scheme on the RNS Basis**
- **Conclusion**
- **References**

Introduction

- **Wireless Sensors Networks (WSN) is one of contemporary direction to develop the fault-tolerant distributed auto-configure systems for monitoring of resources and processes**
- **At the same time the use of WSN in**
 - **Industrial control, safety systems, real-time monitoring systems, and guard systems**
 - **requires high reliability for all levels of OSI model**
- **To improve the data transmission reliability the following approaches are considered there :**
 - **Data Transmission using the Spread-Spectrum methods:**
 - **Direct-Sequencing Spread Spectrum (DSSS), and**
 - **Frequency-Hopping Spread Spectrum (FHSS),**
 - **Error Correction Codes - cyclical redundancy check (CRC)**
 - **Reed–Solomon (RS) codes**
 - **Bose-Chaudhuri-Hocquenghem codes and others [1]**

Introduction (cont-d)

- **Moreover the modified method is proposed [3]**
 - **it's based on extension of signal spectrum by FHSS**
 - **and transformation of Residue Number System**
- **This method enables to implement the noise-eliminating coding and the parallel information processing**
 - **without considerable complication of computing facilities**
- **But the all mentioned approaches above increase the data transmission reliability**
 - **in the WSN physical layer only**

Introduction (cont-d)

- Besides it's still acute a problem for the reliability ensuring and data transmission safety in network layer
- The packet loss in network layer of WSN is caused by units overload, emergency or inaccessibility of units at the modification of the network topology
- In turn the packet retransmission leads to the delay time increase as well as traffics raise and energy costs growing

Existing Methods to Improve the Data Transmission Reliability

- The use of multipath routing is one of the most effective methods to improve the reliability for the data transmission in network layer of WSN [1, 2]
- In multipath routing algorithms the multiple paths are computed per each address,
 - it allows to use rationally the communication channels and increase the overall service capacity
- Moreover the multipath routing provides a simple mechanism to increase a probability of the reliable data delivery for account of the submission a few data duplicates by different routes
- But the use of multipath routing protocols causes may increase energy costs as well as network traffic

Existing Methods to improve the Data Transmission Reliability (cont-d)

- The more effective approach is the algorithm of data sharing on the parts and its transmission by different routes
 - where the Error Correction Code [4] is added per each message part
- The disadvantage of this algorithm is impossibility of message reconstruction if just one part is lost
 - Moreover the WSN limited resources complicate a selection of proper correction codes
- The packet (secret) sharing algorithm is proposed [1, 2]
 - This algorithm is called also as the Threshold Scheme (t, n)
 - where n is a number of parts, in which secret is sharing, and
 - t is a number of parts for secret reconstruction
- In cryptography the following Threshold Schemes are used
 - by Shamir, by Mignotte, by Asmuth-Bloom's [5]

Existing Methods to Improve the Data Transmission Reliability (cont-d)

- The use of existing Threshold Schemes allows to reconstruct data in a case
 - we have t parts, or
 - that is we lose $n - t$ message parts
- In the same time the use of distorted message part may counteract with the data burst reconstruction
- The authors propose therefore
 - the improved method of data burst sharing in WSN based on the RNS,
 - it's described below

Proposed Method of Multipath Routing

- It's proposed to use the Residue Number System to provide sharing the WSN data burst in n parts (sub-packets)
- The sub-packets are created as a result of the residue obtaining after packet division by mutually simple modules p_i ,
 - then the obtained sub-packets are transmitted by different routes

Coding based on Residue Number System

Let's have a system with a basis (p_1, p_2, \dots, p_n)
and a range [6]

$$\mathcal{D} = \prod_{i=1}^n p_i$$

Coding Based on Residue Number System

- It's known, that any number of the range $[0, \wp)$ may be presented in a form of residues choosing the mutually simple basis

$$M = (b_1, b_2, \dots, b_n)$$

This basis system is corresponded uniquely with the following orthogonal bases system

$$B_1, B_2, \dots, B_n,$$

at that a number above in the radix notation can be represented as the

$$M \equiv \sum_{i=1}^n b_i \cdot B_i \pmod{\wp}$$

Coding Based on Residue Number System (cont-d)

The RNS has the following advantages:

- an independence of digit's formation, consequently each digit carries an information about the number as a whole
- a minor digit capacity of residues which are presenting the number
- Rely on the proposed method of multipath routing let's divide the data burst M into shares (t, n) selecting the mutually simple numbers $p_i < p_{i+1}$ which product is (Fig. 1)

$$\prod_{i=1}^t p_i > M$$

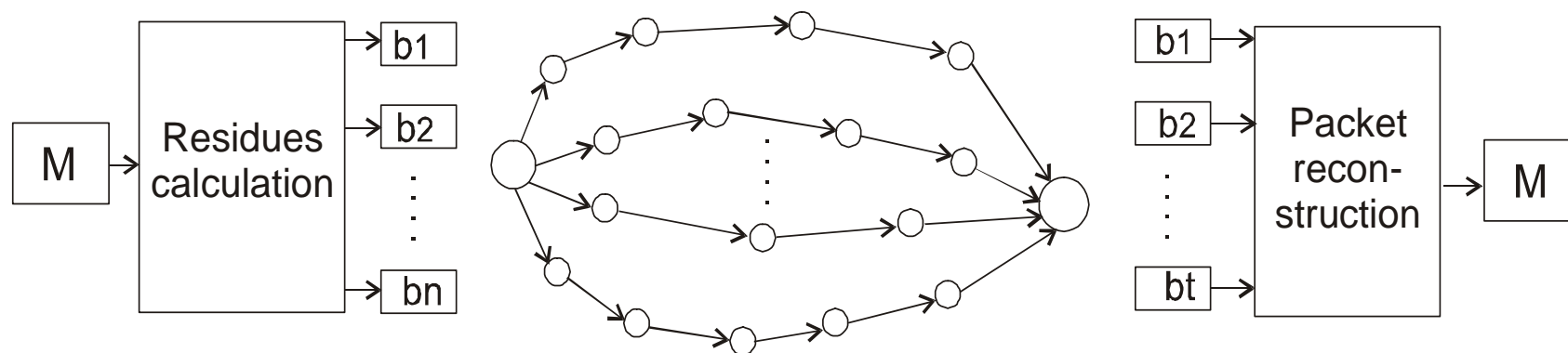
Coding Based on Residue Number System (cont-d)

- Let's divide the data burs into shares

$$b_i = M \bmod p_i$$

and, as a result of sharing, the following data set is formed

$$\{p, p_i, b_i\}$$



Coding Based on Residue Number System (cont-d)

To implement a possibility of data reconstruction by t shares from n let's consider a system with bases

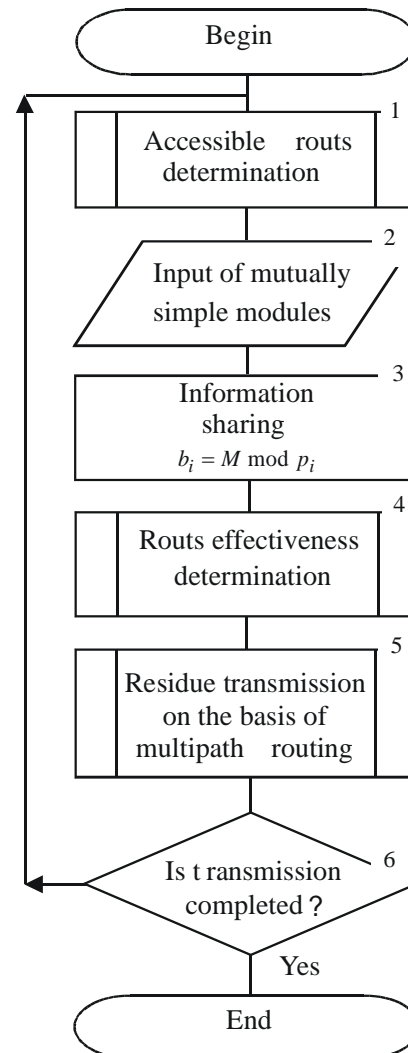
$$p_{t+1}, p_{t+2}, \dots, p_n$$

and a range $p_1, p_2, \dots, p_i, \dots, p_t$ called as a working range. Moreover let's introduce a basis $P = p_1 \cdot p_2 \cdot \dots \cdot p_t$ which are mutually simple with any of the earlier accepted basis, and let's present numbers in the system with basis p_1, \dots, p_n .

It means that we will transfer numbers and make operations at numbers in the wider range $[0, \wp]$, where

$$\wp = P \cdot p_{t+1} \cdot \dots \cdot p_n$$

Multipath Routing Algorithm



Multipath Routing Algorithm (cont-d)

- **The unit WSN activates the data transmission, and determines the accessible nonintersecting routes for the transmission (block 1), and**
 - **evaluates the effectiveness per each route (block 4)**
- **Depending on the number of accessible routes we select the number and values of mutually simple modules (block 2), and**
 - **calculate a working range and a total range of data presentation**
- **As a result of info dividing on selected modules (block 3) we get residues, which are transmitting by determined routes**
- **The bigger residues are transferred by the best quality routs and vice-versa (block 5),**
 - **that permits to improve correcting possibilities of RNS codes and increase the transmission reliability correspondly**
- **A base station receives sub-packets (residues of appropriate modules) and reconstructs initial packets**

Comparative Estimation of Sharing Methods and Experimental Results

- Let's compare the coding redundancy at the information sharing
 - using the existing threshold schemes for the secret sharing
 - Shamir's, Asmuth-Bloom's
 - and the proposed algorithm
- For this purpose we calculate the information volume for the given set points:
 - the number of parts (routes) is $n=10$, $t=8$,
 - a dimension of the data burst is 24 bits

Shamir's Threshold Scheme for Secret Sharing

- A volume of the one share is equal to

$$v_1 = \lceil \log_2 P \rceil + \lceil \log_2 (t - 1) \rceil + \lceil \log_2 t_i \rceil + \lceil \log_2 j \rceil$$

so for the simple number $P > M$

$$v_1 = 57 \quad \text{bits.}$$

Thus data burst with a dimension of 57 bits is formed per each of ten transmission routs.

Asmuth-Bloom's Threshold Scheme for Secret Sharing

- As a result the data set $\{P, p_i, b_i\}$ is formed, and a volume of the one share

$$v_2 = \lceil \log_2 P \rceil + \lceil \log_2 p_i \rceil + \lceil \log_2 b_i \rceil$$

Let's compute the data volume, which is formed as a consequence of the packet division into shares for giving values: $M = 16777216$; at $P > M$ a capacity of is equal 25 bits; a capacity of mutually simple numbers according to the condition $p_i > P$ is also equal at the least 25 bits; a maximum value of residues is equal 25 bits.

So the volume for one share of the message for giving values is 75 bits.

The Coding Scheme on the RNS Basis

- After we applied the RNS transformation the volume of the message one share

$$v_3 = \lceil \log_2 \wp \rceil + \lceil \log_2 p_i \rceil + \lceil \log_2 b_i \rceil$$

To calculate the data volume - which is formed as a result of packet sharing for giving values – let's select the mutually simple modules

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 17,$$

$$p_7 = 19, p_8 = 23, p_9 = 29, p_{10} = 31 \quad \wp = \prod_{i=1}^n p_i = 17160990$$

The Coding Scheme on the RNS Basis (cont-d)

- Since the residues capacity varies depending on the modules value p_i it's reasonable to determine a minimum and a maximum of data volume:

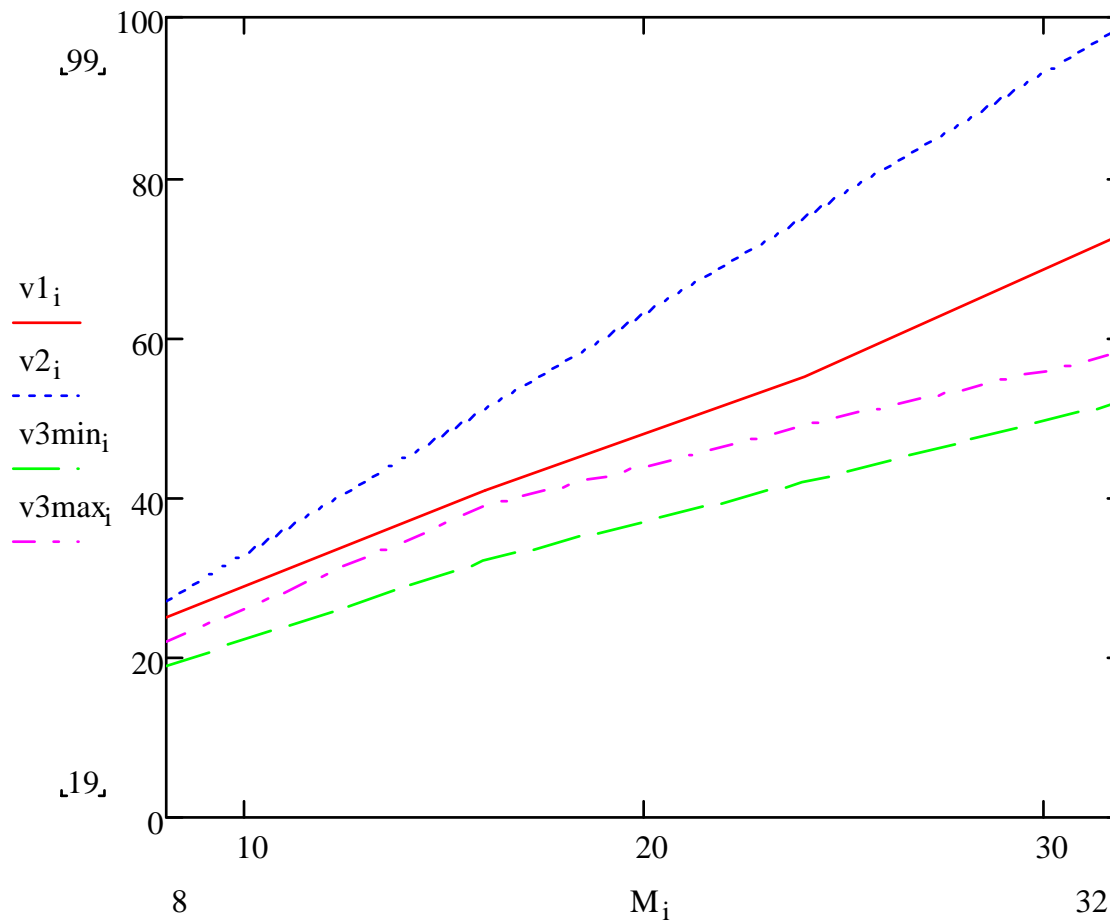
$$v_{3\min} = \lceil \log_2 17160990 \rceil + \lceil \log_2 3 \rceil + \lceil \log_2 2 \rceil = 28 \text{ bits,}$$

$$v_{3\max} = \lceil \log_2 17160990 \rceil + \lceil \log_2 31 \rceil + \lceil \log_2 30 \rceil = 35 \text{ bits.}$$

As it can be seen from the expressions above and Fig.3(see next slide) a proposed method of the message sharing provides a less redundancy in about 1,5 times,

in a comparison with existing methods at the same characteristics of the data reconstruction.

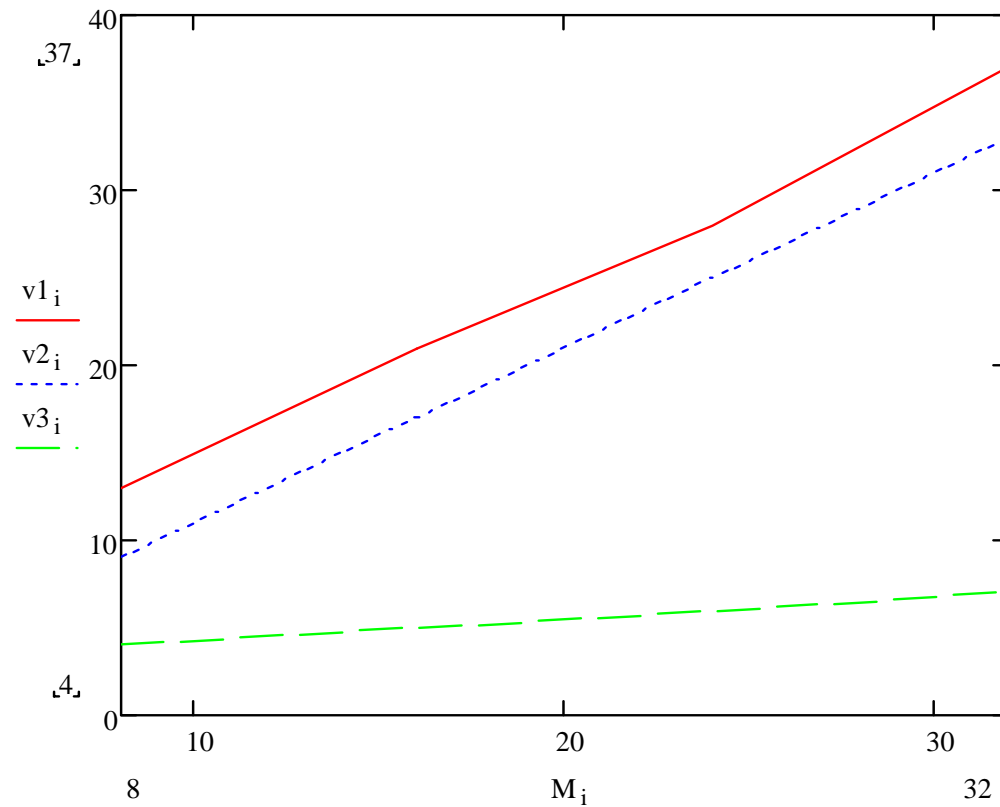
Fig.3 Dependence of data volume v from data burst capacity M for schemes: $v1$ - Shamir's, $v2$ - Asmuth-Bloom's, $v3$ - RNS coding



The Coding Scheme on the RNS Basis (cont-d)

- **It's proofed experimentally:**
 - **to reduce data volumes using the sharing threshold schemes**
 - **we have to transmit variable coefficients only**
- **In this case the constant components**
 - **needed for data reconstruction**
 - **have to be transmitted by the separate packet (Fig.4)**

Fig.4 Dependence of data volume ν from data burst capacity M without accounting of constant components for schemes: $\nu 1$ - Shamir's, $\nu 2$ - Asmuth-Bloom's, $\nu 3$ - RNS coding



Conclusion

- A method of the message sharing based on the residue number system was proposed,
 - it provides less redundancy in comparison with threshold schemes of the secret sharing:
 - in 1,5 times less redundancy in a case of service data transmitting per each part of packet
 - in 5 times less redundancy in a case of service data transmitting by the separate packet
- Once more advantage:
 - sub-packets (residues) of the different capacity are formed after a message was shared,
 - it allows distributing the sub-packets (residues) depending on the integrated estimation of the route quality

References

- 1. W. Lou, “An efficient N-to-1 multipath routing protocol in wireless sensor networks”, Proceedings of IEEE international Conference on Mobile Ad-hoc and Sensor Systems (MASS), Washington, DC, November 2005.
- 2. Zhukov I. A., Drovovozov V. I., Methods of increasing of reliability and data collection safety in real time control systems //The issues of information and control, 1(23). – 2008. – Pp. 262– 276. (In Russian)
- 3. A. Sachenko, V. Yatskiv, R. Krepych. Modified Method of Noise-Immune Data Transmission in Wireless Sensors Networks // International Conference on Networks Security, Wireless Communications and Trusted Computing, “NSWCTC 2009”, 25-26 April 2009, Wuhan, Hubei, China, Volume 2, Pp.847–850.
- 4. W. Lou, W. Liu, Y. Fang, “SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004.
- 5. Bruce Schneier. Applied cryptography: protocols, algorithms, and source code in C. – M.: Triumph, 2002. – 816 p. (In Russian)
- 6. Modular Parallel Computing Structures of Neuro Processing System / N. I. Chervyakov, P. A. Sakhnyuk, A. V. Shaposhnikov, S. A. Ryadnov. Edited by N. I. Chervyakov. – M.: Fizmatlit, 2003. – 288 p. (In Russian)

Thank you for your attention !