sensors

MDPI

Article

DT-RRNS: Routing Protocol Design for Secure and Reliable Distributed Smart Sensors Communication Systems †

Andrei Gladkov [1], Egor Shiriaev [1], Andrei Tchernykh [2,3,*], Maxim Deryabin [4], Mikhail Babenko [5] and Sergio Nesmachnow [6]

[1] Faculty of Mathematics and Computer Science, North-Caucasus Federal University, 355017 Stavropol, Russia
[2] Computer Science Department, CICESE Research Center, Ensenada 22860, Mexico
[3] Control/Management and Applied Mathematics, Ivannikov Institute for System Programming, 109004 Moscow, Russia
[4] Computing Platform Lab, Samsung Advanced Institute of Technology, Suwon 16678, Republic of Korea
[5] North-Caucasus Center for Mathematical Research, North-Caucasus Federal University, 355017 Stavropol, Russia
[6] Faculty of Engineering, Universidad de la República, Montevideo 11300, Uruguay
* Correspondence: chernykh@cicese.mx; Tel.: +52-646-1786994

† This paper is an extended version of "Secret Sharing Scheme for Security of Smart City Communication Systems". In Proceedings of the V Ibero-American Congress of Smart Cities (ICSC-CITIES 2022), Cuenca, Ecuador, 28–30 November 2022.

Abstract: A smart city has a complex hierarchical communication system with various components. It must meet the requirements of fast connection, reliability, and security without data compromise. Internet of Things technology is widely used to provide connectivity and control solutions for smart sensors and other devices using heterogeneous networking technologies. In this paper, we propose a routing solution for Wireless Sensor Networks (WSN) and Mobile Ad hoc NETworks (MANET) with increasing speed, reliability, and sufficient security. Many routing protocols have been proposed for WSNs and MANETs. We combine the Secret Sharing Schemes (SSS) and Redundant Residual Number Systems (RRNS) to provide an efficient mechanism for a Distributed dynamic heterogeneous network Transmission (DT) with new security and reliability routing protocol (DT-RRNS). We analyze the concept of data transmission based on RRNS that divides data into smaller encoded shares and transmits them in parallel, protecting them from attacks on routes by adaptive multipath secured transmission and providing self-correcting properties that improve the reliability and fault tolerance of the entire system.

Keywords: smart city; Residue Number System; Secret Sharing Schemes; distributed transmitted; reliability; Mobile Ad hoc Network; communication; heterogeneous sensor networks

Citation: Gladkov, A.; Shiriaev, E.; Tchernykh, A.; Deryabin, M.; Babenko, M.; Nesmachnow, S. DT-RRNS: Routing Protocol Design for Secure and Reliable Distributed Smart Sensors Communication Systems. *Sensors* **2023**, *23*, 3738. https://doi.org/10.3390/s23073738

Academic Editor: George Ghinea

Received: 4 March 2023
Revised: 28 March 2023
Accepted: 30 March 2023
Published: 4 April 2023

1. Introduction

Internet of Things (IoT) technology for a smart city is widely used to provide solutions for connecting smart things using heterogeneous networks and advanced communication technologies.

As the main assets, various city systems, objects, and sensors can act as distributed information systems generating data, i.e., power plants, schools, transport, law enforcement agencies, hospitals, and other public services. The main objective is to improve the living standard and urban service quality. The information gained from smart sensors allows us to analyze and manage the urban environment in real-time with a quick response. There are many scientific, commercial, and governmental solutions for implementing a smart city concept.

According to Deakin's generalized definition [1], a smart city is a city that uses an information system to meet the needs of city residents. It is not only a set of technological solutions but is the application of these technologies by local communities.

Let us consider the main hardware components of the smart city network. It consists of many elements, including video surveillance, emergency call systems, biometric systems, city and banking services, intelligent transport, and IoT solutions (Radio Frequency Identification [2,3], sensors for measuring temperature, humidity, illumination, pressure, etc.). Smart sensor networks play a substantial role in IoT. Their components include sensing, data collection, heterogeneous connectivity, data processing, etc. [3–5].

Large-scale data sharing in a distributed environment is fraught with data security and privacy issues, as data being compromised can harm people and the entire system. Another important aspect is reliability [3]. Failures can delay the response of emergency systems, medical, and rescue services. Thus, when building a smart city communication infrastructure, design methods that provide data security at the required level while having high reliability and speed are very important.

In [6], we propose combining the Secret Sharing Schemes (SSS) and Redundant Residual Number Systems (RRNS) as an efficient security mechanism for a smart city dynamic heterogeneous network and show how RRNS increases communication reliability through effective correcting management.

This paper presents a more extensive and in-depth study of data transmission in the proposed DT-RRNS protocol. We propose a routing solution for the Wireless Sensor Network (WSN) and Mobile Ad hoc NETwork (MANET) and present a methodology for ensuring the security and reliability of data transmission.

The method is based on Node-Disjoint Multipath Routing [5], which allows to exchange and manage data between smart things, ensuring privacy by the threshold SSSs and Redundant Residue Number System (RRNS). We describe details of the generation of parameters that overcome the limitations of the well-known Mignotte scheme, data partitioning, and data recovery and provide a theoretical analysis of reliability and security bounds.

We consider the network as a distributed infrastructure rather than a centralized system. It is well known that for large networks, centralized data processing imposes a large load on the central computing bottleneck slowing down the entire system. More detailed arguments about the positive and negative properties of a decentralized network can be seen in [7–9].

SSS is a cryptographic technique that splits a secret into several shares $s = \{s_1, s_2, \ldots, s_n\}$ and distributes them among participants. In the most used (k, n) threshold SSS, a combination of k shares from n is needed to recover the secret, where $k \leq n$.

RRNS is one of the most common non-positional number systems that represents the number of a positional system as a tuple of n numbers $(s_1, s_2, \ldots, s_n)$, obtained by dividing numbers into residuals (see Section 4). Among many of its applications, we could mention the acceleration of operations due to the parallel implementation of basic arithmetic, information integrity control, digital signal processing, etc.

This paper is structured as follows: Section 2 considers data transmission in smart city IoT networks. Section 3 discusses existing approaches to ensure security, as well as the advantages of distributed SSS schemes based on RRNS. Section 4 describes the RRNS and SSS details. Section 5 discusses the proposed DT-RRNS. Section 6 presents the proof of correctness and discusses the main properties of the proposed scheme, its security, and its reliability. Section 7 discusses a generalized scheme and principles for secure and reliable data transmission. Section 8 analyzes data transmission security. Section 9 provides a performance analysis. Section 10 presents the main conclusions and future work.

2. Data Transmission in IoT Networks

A wireless ad hoc network and MANET are important concepts of smart city communication. It is widely used for ensuring self-configuring and dynamic connectivity between sensors, humans, and devices that send and receive information.

Lobo et al. [10] study the Quality of Service of MANET in smart city networks with an emphasis on healthcare. Several frameworks were considered that improve the transmission quality of MANET, as well as individual elements, such as video signal transmission.

Cardone et al. [11] discuss the MANET and WSN hybrid network for fast data collection in the smart city. The authors provide a transmission protocol based on modern data transmission standards considering IPv6. Pandey et al. [12] study methods to improve the reliability of MANET networks and propose a method of self-healing nodes.

In this work, our goal is to increase the speed and reliability of MANET communication to ensure security. To achieve this goal, we propose the use of RRNS in MANET.

In the original version, MANET solves the minimax optimization problem of finding the shortest path in the network. The smart city network can be represented as a directed graph, where the vertices are the communication nodes (devices in the network), and the arcs are the data transmission between the nodes. Let us establish that $G(V, E)$ is a network graph with a flow $v_0 \in V$ and path cost function $c : E \to R$. We assume that the set of vertices V split into two non-overlapping subsets V_A and V_B ($V_A \cup V_B = V, V_A \cap V_B = \varnothing$).

Now, we fix a pair of mappings:

$$s_A : v \to V_G(v) \; for \; v \in V_A \backslash \{v_0\}; \; s_B : v \to V_G(v) \; for \; v \in V_B \backslash \{v_0\}; \tag{1}$$

where $V_G(v)$ is the set of ends of all arcs outgoing from a vertex v. We define the following subgraph $T_s = (V, E_s)$, generated by a set of arcs of the form $(v, s_A(v))$ and $(v, s_B(V))$. This subgraph has the property that for some given vertex $w \in V$, or there is a way $P_T, (w, v_0)$ from w to v_0.

For an arbitrary vertex, $w \in V$ defines the value $\widetilde{c}(s_A, s_B, w)$ as the sum of the costs of the arcs of the path $P_T, (w, v_0)$, if such a path exists in T_s. If the path $P_T, (w, v_0)$ does not exist in T_s, we assume the value $\widetilde{c}(s_A, s_B, w)$ equals to ∞ or $-\infty$ depending on the positivity and negativity of the sum of the costs of the arcs of the oriented cycle C_w.

If the sum of the costs of the arcs of an oriented cycle C_w is zero, then $\widetilde{c}(s_A, s_B, w)$ equals the sum of the costs of the arcs of the path connecting the vertex w with the cycle C_w. That is, a problem is formulated as $F(w) = \min\limits_{s_A} \max\limits_{s_B} \widetilde{c}(s_A, s_B, w)$.

Let us consider the data transmission model presented in Figures 1 and 2. It is known that MANET transmits data using devices located on the infrastructure-less, distributed wireless networks without static-located transmission stations. It is an interesting and promising solution providing communication of a big variety of devices, from mobile devices to personal cars, from smart devices to public transport, etc. In addition, a smart city infrastructure also contains static nodes, such as data centers, storage, decision centers, etc.

For such a dynamic heterogeneous network, we propose the concept of parallel data transmission based on RRNS that divides data into smaller shares and transmits them in parallel. The self-correcting properties of RRNS can improve the reliability and fault tolerance of the entire system [13–16].

Figure 1 shows a conceptual model described above. We group the elements of a smart city according to common features. They can be separated from each other by large distances and distributed like data management modules.

This model gives a general idea of the transmission network complexity. Each group of components is connected to other groups, and control devices can communicate with any device on the network. In such a data transmission model, MANET provides a definite advantage. Devices, such as sensors, can send data to a destination, transmitting it through other devices within the network.

Figure 2 shows the data transmission from the sensor to the recipient in the DT model. The recipient can be a data warehouse, decision center, data processing center, cloud data analysis, etc. RRNS transmits data in the MANET network in parallel breaking the message into several shares. It improves the speed at which data are transmitted across communication channels since such shares are smaller than the original message.

We use the term Weighted Number System (WNS) as a traditional positional decimal number system.

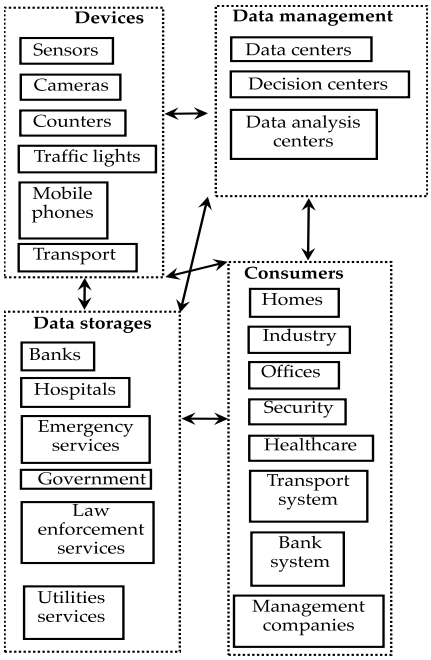

Figure 1. The general model of data transmission.

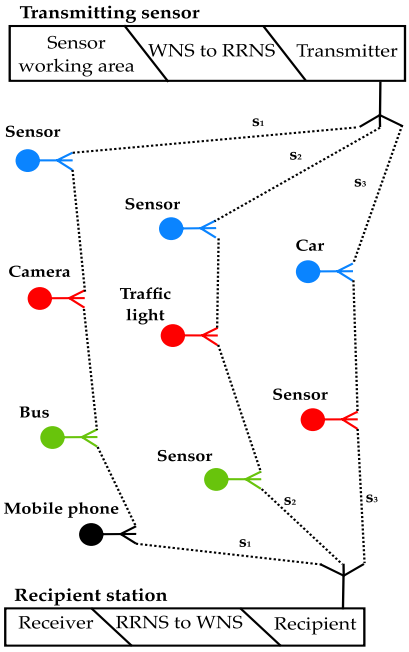

Figure 2. Distributed data transmission model.

Figure 3 shows the model of data transmission packets. The receiver collects shares of information and combines them. The application knows how many shares have arrived and how many shares should arrive. RRNS has self-correcting properties for recovering the message if one or several shares are lost or intentionally changed. If arrived shares are not enough, it waits a certain time, and the packet is requested again or ignored. As a result, we can have a network with increasing speed and reliability.

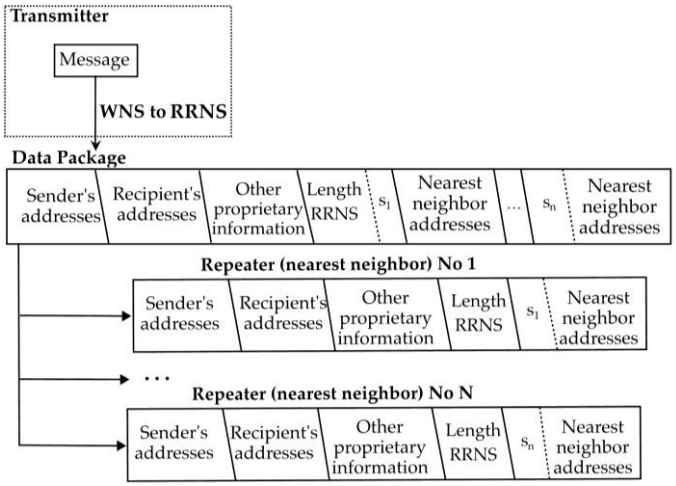

Figure 3. Data packet model.

3. DT Security and Reliability

Our main approach is to use RRNS to ensure the security of data transmission. Let us discuss and compare well-known solutions for providing reliability and security of distributed data storage and transmission. Four main methods are used to ensure reliability [17]: Replication, Erasure code, Erasure code modifications, and Error correction code.

Chang et al. [18] presented a modified data replication method, providing a high encoding and decoding speed. However, it requires additional cryptographic primitives to ensure security and has a high redundancy compared to erasure codes.

Many different modifications of erasure codes have been proposed to create reliable methods for DT. The joint use of error correction and erasure codes maintains system performance and minimizes the load on the data transmission network when recovering lost fragments [19,20].

Erasure codes based on the RRNS [21] allow data to be processed in the encoded form [14]. So, it can be used both in the design of low-power wireless data transmission devices and DT.

Secure DTs are based on the use of cryptographic primitives—symmetric encryption algorithms (AES) and digital signatures based on RSA (Rivest, Shamir, Adleman) [22]. The advantages of these approaches are high speed of encryption and decryption and low data redundancy. The disadvantage is that an error in the encrypted data leads to its loss. To eliminate this shortcoming, the use of additional mechanisms for accessing data for a long time is required [23].

When building secure and reliable DT, the following methods are used: elliptic cryptography and erasure codes [24,25], access structures [26,27], error correction codes [28,29], graph-based algorithms and modified data replication algorithm [30], attribute-based encryption [31], etc.

An alternative approach is to use recovery codes [20], erasure codes, and error correction codes based on RRNS [19]. However, recovery codes and erasure codes do not allow encoded data processing. Homomorphic calculations process encoded data without additional computational costs for decoding.

A significant breakthrough in the field of homomorphic computing came from the work of Gentry [32]. The authors proposed a fully homomorphic scheme to perform both addition and multiplication. The main disadvantages of this algorithm are significant data redundancy and lack of control over the results of arithmetic operations.

Particular attention should be paid to the distributed data storage model proposed in [33], guaranteeing security, privacy, homomorphism, reliability, and scalability. The authors propose two approaches to building systems based on homomorphic access structures in RRNS, with RRNS moduli being used as secret keys stored by users. Data processing

leads to an exponential increase in the load on the network and memory, which makes this model inapplicable in practice in modern conditions.

Access structures [34,35] ensure data security and confidentiality. RRNS implements the same functionality as the Mignotte scheme but allows you to control the results of data processing. DT is also characterized by collusion risks [36]. Several approaches have been developed to prevent cloud collusion [26]. As mentioned above, the non-stationarity of the cloud environment reduces the efficiency, performance, reliability, and security of the system. The adaptive paradigm reduces uncertainty but is rarely used in cloud computing [36].

Let us consider the following scenario. The user has confidential data and decides not to send it using a single path. He divides them into several shares and transmits them in different paths between nodes. There are several types of security threats in this scenario.

Deliberate threats include unauthorized access to information, interception, falsification, hacker attacks, etc., in one or more nodes.

Random threats include errors, crashes, etc. They can lead to the loss of one or more shares of data, inconsistencies between different copies of the same data, and/or the inability to recover the original data. Collusion threats are illegal agreements between two or more adversaries (in the context of different paths between nodes, the adversaries are nodes) to gain full access to personal data. Cryptographic protocols can be used to mitigate the risks of deliberate threats, but this is not enough for random threats.

We consider reliability and security as close concepts of an information violation. Therefore, statements related to reliability are used to discuss security and vice versa.

To improve the security and reliability of data transmission systems, DT is based on access structures and error correction codes. It transmits data through various paths between nodes and minimizes the chance of information theft or loss in case of intentional and accidental threats.

In the next sections, we show how the size of shares and their number can change the reliability, security, speed, etc. of data transmission. These structures reduce the load on the transmission network compared to the classical replication mechanism and reduce the cost.

4. Residue Number System and Secret Sharing

$(k,\ n)$-RRNS is determined by a system of pairwise coprime moduli $\{p_1, p_2, \ldots, p_n\}$. Positional integer number s such that $0 \leq s < P$, where $P = \prod_{i=1}^{k} p_i$, is represented as a tuple of n numbers $s \overset{RRNS}{\rightarrow} (s_1, s_2, \ldots, s_n)$, where $n = k + r$ and

$$s_i = s \bmod p_i,\ i = 1, 2, \ldots, n. \tag{2}$$

RRNS is a redundant representation of the Residue Number System (RNS). Redundancy is represented by additional moduli in the moduli set. k is the RNS dimension; r is the dimension of redundant moduli; and n is the RRNS dimension. According to the RRNS property, if the number of moduli is r, then it can detect r and correct $\lfloor r/2 \rfloor$ errors.

Redundancy supports reliable data processing and transmission systems with multiple error detection and correction. To detect and correct errors in RRNS, several methods are used, for instance, syndrome and projection methods [28,29]. If we consider RRNS not only as the error detection, localization, and correction code but also as the Mignotte SSS, then we can conclude that RRNS ensures data security.

RRNS has many applications because of its properties such as parallelism and modularity, among which we can mention hardware and software acceleration, information integrity control, digital signal processing, increasing the robustness of information transmission between computers, etc.

Modular calculus is based on the Chinese Remainder Theorem (CRT) [28], according to which the number s can be uniquely calculated by the formula

$$s = \left| \sum_{i=1}^{k} \left| P_i^{-1} \right|_{p_i} P_i s_i \right|_P, \quad (3)$$

where $P_i = \frac{P}{p_i}$, $\left|P_i^{-1}\right|_{p_i}$—multiplicative inversion P_i modulo p_i, for $i = 1, 2, \ldots, k$.

This method is called the CRT method or the Garner method. However, it is computationally complex, since it requires division by a sufficiently large number P. It is worth noting that there are many well-developed methods for an efficient implementation of calculating the remainder of the division and converting numbers back from RRNS to a WNS. It makes this system suitable for use as the basics of a SSS [15,26,28].

Let us consider SSSs using Shamir's threshold scheme as an example [27]. The idea of this scheme is that the secret is represented as a polynomial $k-1$ degrees. Then, to interpolate the resulting polynomial, it is necessary k points, and the polynomial can be divided into n shares. Then, the secret-sharing process is as follows. Let we need to divide the secret s on n shares. To do this, take a prime number $p > s$. The following polynomial is constructed:

$$F(x) = \left(a_{k-1} x^{k-1} + a_{k-2} x^{k-2} + \ldots + a_1 x + s \right) \bmod p, \quad (4)$$

where $a_{k-1}, a_{k-2}, \ldots, a_1$—random numbers that are only known when the secret is shared.

The secret recovery occurs due to the calculation of the Lagrange interpolation polynomial according to the following formula:

$$F(x) = \sum_i l_i(x) y_i \bmod p; l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \bmod p, \quad (5)$$

where (x_i, y_i)—polynomial point coordinates. In addition, there is a limitation: all calculations are performed only in the final field p. In this scheme, an integer polynomial is used. Despite the low redundancy and high scalability, the field space p is not used efficiently.

This scheme was developed by Hugo Krawczyk in 1993 [37]. In this scheme, integer coefficients are shares. It is a (k, n) threshold SSS. It distributes s among k participants randomly. The recovery of the secret is possible from k shares, while $k-1$ shares do not allow you to recover s.

Let us consider the Information Dissemination Algorithm designated as IDA (Algorithm 1). This algorithm works for parameters n (total number of shares) and k (required number of shares for recovery). It includes a secure encryption function with a private key, which is designated as ENC. In addition, the algorithm implements a computationally secure (k, n) SSS. It is also worth noting that the space of both the secret and the message in this scheme is the same as for the encryption function ENC.

Algorithm 1. Secret Sharing of Krawczyk scheme.

1. Choosing a random encryption key K; secret s is encrypted by ENC, $e = \mathrm{ENC_K(s)}$.
2. e is divided into n fragments—e_1, e_2, ..., e_n by the scheme.
3. K is represented as a tuple of n numbers K_1, K_2, ..., K_n by Asmuth-Bloom SSS.
4. Shares $m_\mathrm{i} = (e_i, K_\mathrm{i})$, $i = \overline{1, n}$ are distributed between participants

In Algorithm 2, every share m_i has a bit length $|e_i| + |K_i|$, where $|x|$ is a bit number of x. Evidence of this, as well as confirmation of the secrecy of the scheme, is given in [38].

Algorithm 2. Secret Recovery of Krawczyk scheme.

1. k participants combine their shares $m_{i_j} = \left(e_{i_j},\ K_{i_j}\right)$ with indexes $\{i_1, i_2, \ldots, i_k\}$ together
2. e is recovered from shares e_{i_j}.
3. key K is recovered from K_{i_j} by Asmuth-Bloom
4. Using K, e is decrypted then s is recovered.

Despite the obvious advantages of these schemes (low redundancy, scalability, flexibility), they have several disadvantages, such as the inability to add new participants without recovering the secret and re-sharing it which is important for smart city infrastructure. The advantages and limitations of the DT-RRNS scheme are discussed in the next sections.

5. Secret Sharing Scheme with Residue Number System

In this section, we introduce the basic concepts of security of two well-known SSS based on RRNS: Asmuth-Bloom and Mignotte.

Let each participant have a unique number or identifier. The entire set of these numbers we call the universal set of numbers and denote U (in the simplest case $U = \{1, 2, \ldots, n\}$, where n is the number of participants in the scheme).

The set of authorized (qualified) coalitions is called the authorized subsets of U denoted by I. Participants of the qualified subsets can recover the secret from their shares when they act together to pool their knowledge.

An unauthorized subset is a subset $\widetilde{I}$ of participants of any coalition that does not have the right to recover the secret.

In the Asmuth-Bloom scheme, p_0 is a secret key, and $s \in [0, p_0)$. The moduli $p_1 < p_2 < \ldots < p_k < p_{k+1} < \ldots < p_n$ have to be chosen, so that $\prod_{i=1}^{k} p_i > p_0 \prod_{i=0}^{k-2} p_{n-i}$. The last inequality is usually called the Asmuth-Bloom condition. At the stage of sharing the secret, a random number r_n is generated such that $s' = s + r_n p_0 < \prod_{i=1}^{k} p_i$.

Secret s' is divided so that $s_i = s' \bmod p_i$ is a share for participant i, where $i = 1, 2, \ldots, n$. Any set of authorized participants with numbers from I can recover the secret; wherein $n \geq |I| = m \geq k$.

Using the CRT, s' is recovered based on its RRNS representation $\left(s_{i_1}, s_{i_2}, \ldots, s_{i_m}\right)$ with moduli $p_{i_1}, p_{i_2}, \ldots, p_{i_m}$, where $i_j \in I$, for all $j = 1, 2, \ldots, m$. s is recovered as the remainder of the division of s' on p_0: $s = s' \bmod p_0$.

Let us consider an unauthorized coalition of participants with numbers from $\widetilde{I}$. Then $\left|\widetilde{I}\right| \leq k - 1$, let $P = \prod_{i=1}^{k} p_i$ and $\widetilde{P} = \prod_{i \in \widetilde{I}} p_i$. In this case, $\widetilde{s} = s' \bmod \widetilde{P}$. According to the Asmuth-Bloom conditions $P/\widetilde{P} > p_0$ and $\left(\widetilde{P}, p_0\right) = 1$. Thus, as shown in [34], an unauthorized coalition obtained fewer than k shares does not receive any useful information about the secret.

In the Mignotte $(k,\ n)$ threshold scheme, moduli $p_1 < p_2 < \ldots < p_k < p_{k+1} < \ldots < p_n$ are chosen to satisfy the inequality:

$$\alpha = \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i = \beta. \tag{6}$$

To achieve security, secret s has to be in the interval (α, β). Any set I of authorized participants can recover the secret, wherein $|I| = m \geq k$. s is recovered by CRT using $\left(s_{i_1}, s_{i_2}, \ldots, s_{i_m}\right)$ and moduli $p_{i_1}, p_{i_2}, \ldots, p_{i_m}$, where $i_j \in I$, for all $j = 1, 2, \ldots, m$.

To ensure security, Mignotte sequences with a large value $(\beta - \alpha)/\beta$ should be used [35]. This scheme is not computationally secure but has practical applications due to reduced redundancy compared with Asmuth-Bloom.

Let us consider the concept of entropy, which plays an important role in SSS security theory.

We denote the entropy of the secret as $H(s) = \log_2 s$. In this case, the entropy is maximum. Knowing the subset of the shares $s^* = \left(s_{i_1}, s_{i_2}, \ldots, s_{i_m}\right)$, we denote entropy

as $H(s^*, I) = \min(\log_2 s, \sum_{i\in I} \log_2 p_i)$, where $\forall j : i_j \in I$ and $|I| = m$. If I is the set of authorized participants, then $H(s^*, I) = H(s) = \log_2 s$. The important characteristic of the SSS is the uncertainty of the secret that is defined by

$$\Delta(s, s^*, I) = H(s) - H(s^*, I). \tag{7}$$

SSS is computationally secure if $\Delta\left(s, s^*, \overline{I}\right) = H(s)$ for all $\overline{I}$, where $\overline{I}$ is the set of unauthorized participants. For the set of authorized participants, the secret can be recovered correctly; hence, the uncertainty is equal to:

$$\Delta\left(s_i : i \in \widetilde{I}\right) = 0. \tag{8}$$

To analyze the security of SSS based on RRNS, an additional concept of the perfect SSS was introduced in [38]. SSS is called perfect if any unauthorized subset participants cannot obtain any information about the secret. Hence, the scheme is perfect if, for all unauthorized subsets of participants with numbers $\widetilde{I}$ and for any $\varepsilon > 0$, there is s, such that, for $p_0 < p_1 < \ldots < p_n$, $p_i > s$ $(i = 0, 1, \ldots, n)$, and $\Delta\left(s, s^*, \overline{I}\right) < \varepsilon$.

The scheme is called ideal if the space of share has the same dimension as the secret space. An ideal SSS is perfect with the smallest possible size of each share.

The question of how exactly it is necessary to choose the parameters of the SSS on the RRNS so that it has the asymptotic idealness property remains open. In [38], the authors show the asymptotic idealness of the Asmuth-Bloom scheme using "sufficiently close" coprime numbers for RRNS moduli. The work [39] considers so-called compact sequences of coprime numbers with an initial value p_0 when $p_n < p_0 + p_0^\theta$ for some real number $\theta \in (0, 1)$. In the following analysis, we assume that the compact sequences of coprime numbers are used as the moduli sets.

Let us now consider the concept of computationally secure SSS. Assume that at some point in time, unauthorized participants collect several shares with numbers $\widetilde{I}$. The objective of the unauthorized participants is to recover the secret based on the available data.

Let S be a universal set of all subsets of possible secrets recovered from all available shares. S can be divided into two subsets. First subset S_1 consists of all possible secrets that cannot be used to obtain the secret. The second subset S_2 contains all remaining possible secrets. For example, if the Mignotte scheme knows the share of the secret s_j for modulo p_j, $0 \le j \le n$, then the secret must satisfy the condition: $s \equiv s_j \bmod p_j$. Therefore, in this case, $S_1 = \{s : s \in S \wedge s \not\equiv s_j \bmod p_j\}$ and $S_2 = \left\{s : s \in S \wedge s \equiv s_j \bmod p_j\right\}$. Note that if the SSS is perfect, then $S_1 = \varnothing$ and $S_2 = S$.

Thus, to obtain the original secret, it is necessary to use all combinations of indexes included in S_2 and the security of the scheme depends on the cardinality of this set and the computational complexity of the complete permutation.

It is necessary to generate the scheme parameters in such a way that unauthorized participants cannot, using modern computing resources, obtain the secret in a reasonable time. A scheme that meets these conditions is called a computationally secure scheme. As a measure of computationally secure, we take the cardinality of the set S_2: $f(\widetilde{I}) = |S_2|$.

For the Asmuth-Bloom scheme, considering its asymptotic idealness, and Asmuth-Bloom condition, $f(\widetilde{I}) = |S| \le p_0$ for $\widetilde{I}$.

Computationally secure schemes are not always ideal but have reduced redundancy, which is important in practical applications.

6. Data Transmission Security and Reliability

Let us consider parameter generation, secret sharing, and secret recovery for threshold (k, n)-DT-RRNS.

Parameter generation. A compact sequence of coprime numbers is selected $p_1 < p_2 < \ldots < p_k < p_{k+1} < \ldots < p_n$; where $p_n < p_1 + p_1^\theta$ and $\theta \in (0, 1)$; secret $s \in [0, P)$, where $P = \prod_{i=1}^{k} p_i$ is the dynamic range of the RRNS.

Secret Sharing. Shares s_i of a secret s are calculated as $\forall\, i = \overline{1,n} : s_i = s \bmod p_i$.

Secret Recovery. Any authorized set of participants with numbers I can uniquely recover the secret, where $|I| = m \geq k$. s is calculated using CRT $s = \left| \sum_{j=1}^{m} s_{i_j} P_{j,m} \left| P_{j,m}^{-1} \right|_{p_{i_j}} \right|_M$, where $M = \prod_{j=1}^{m} p_{i_j}$ and $P_{j,m} = M/p_{i_j}$.

Let us consider the main properties of the DT-RRNS. The following notations are introduced.

I	Authorized set is subset of $\{1, 2, \ldots, n\}$, cardinality is equal to k
$\widetilde{I}$	Unauthorized set is subset $\{1, 2, \ldots, n\}$, cardinality is less to k
$\widetilde{I}_{max}$	Unauthorized set $\{n-k+2,\ n-k+3, \ldots, n\}$ cardinality is equal to $k-1$
$\widetilde{P} = \prod_{i \in \widetilde{I}} p_i$	Dynamic range for an unauthorized set $\widetilde{I}$
$\widetilde{P}_{max} = \prod_{i \in \widetilde{I}_{max}} p_i$	Dynamic range for an unauthorized set $\widetilde{I}_{max}$
$f\left(\widetilde{I}\right)$	Cardinality of the set of possible secrets $\widetilde{s}$ for a given $\widetilde{P}$
$f\left(\widetilde{I}_{max}\right)$	Cardinality of the set of possible secrets $\widetilde{s}$ for a given $\widetilde{P}_{max}$
$\widetilde{s} = s \bmod \widetilde{P}$	Projection of the secret s modulo $\widetilde{P}$
f_k	Approximate value of $f\left(\widetilde{I}\right)$
S	Universal set of all subsets of possible secrets recovered from all available shares
Q_i	The probability of intercepting i nodes
R	Proximity of the cardinality of possible secrets $f\left(\widetilde{I}_{max}\right)$ to p_1

The following statement shows a lower bound for the moduli selection.

Statement 1. *In DT-RRNS, for any unauthorized subset of participants with numbers* $\widetilde{I}$, $P > \widetilde{P} = \prod_{i \in \widetilde{I}} p_i$ *and* $p_1 > 2^{k-1}$.

Proof. Using the fact that in threshold SSS the maximum unauthorized subset is the subset numbered $n, n-1, \ldots, n-k+2$ and considering the definition of compact sequences, we obtain:

$$\widetilde{P} < \prod_{i=0}^{k-2} p_{n-i} < \left(p_1 + p_1^{\theta}\right)^{k-1} = p_1^{k-1}\left(1 + p_1^{\theta-1}\right)^{k-1} < p_1^{k-1} 2^{k-1}. \tag{9}$$

On the other hand, $P > p_1^k$. From here

$$\frac{P}{\widetilde{P}} > \frac{p_1^k}{p_1^{k-1} 2^{k-1}} = \frac{p_1}{2^{k-1}} \tag{10}$$

To comply with the condition $P > \widetilde{P}$ it is necessary to fulfill the inequality $P/\widetilde{P} > 1$. This inequality will necessarily hold if the inequality $\frac{p_1}{2^{k-1}} > 1$, or which is equivalent, $p_1 > 2^{k-1}$. The statement is proven. □

In other words, the DT-RRNS is applicable when choosing a module p_1 at the parameter generation stage such that $p_1 > 2^{k-1}$.

Statement 2. *For DT-RRNS, when combining the shares of an unauthorized subset of participants of* $\widetilde{I}$, *the cardinality of the enumeration set* $f\left(\widetilde{I}\right)$ *is determined by the expression:*

$$\left\lfloor \frac{P}{\widetilde{P}} \right\rfloor \leq f\left(\widetilde{I}\right) \leq \left\lfloor \frac{P}{\widetilde{P}} \right\rfloor + 1, \tag{11}$$

where $\widetilde{P} = \prod_{i \in \widetilde{I}} p_i$.

Proof. Since the shares, whose numbers belong to $\widetilde{I}$, are known, then for all p_{i_j} such that $i_j \in \widetilde{I}$, it is possible to recover the number $\widetilde{s} \equiv s \bmod \widetilde{P}$ due to $s = a\widetilde{P} + \widetilde{s}$. The only unknown secret parameter is $a \in \mathbb{Z}$.

Let us define the upper and lower bound of a.

s is defined with dynamic range P. Consequently $0 \le a\widetilde{P} + \widetilde{s} \le P - 1$, where

$$-\frac{\widetilde{s}}{\widetilde{P}} \le a \le \frac{P - \widetilde{s} - 1}{\widetilde{P}}. \tag{12}$$

Taking into account that s and a are non-negative and since $\widetilde{s} < \widetilde{P}$ and $\left\lfloor \frac{P}{\widetilde{P}} \right\rfloor - 1 < \frac{P-\widetilde{s}-1}{\widetilde{P}} < \left\lfloor \frac{P}{\widetilde{P}} \right\rfloor + 1$, $\left\lfloor \frac{P}{\widetilde{P}} \right\rfloor - 1 \le \left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor \le \left\lfloor \frac{P}{\widetilde{P}} \right\rfloor$. We have

$$0 = -\left\lceil \frac{\widetilde{s}}{\widetilde{P}} \right\rceil \le a \le \left\lfloor \frac{P - \widetilde{s} - 1}{\widetilde{P}} \right\rfloor. \tag{13}$$

That is, a lies in between $\left[0, \left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor\right]$, whose cardinality is $f\left(\widetilde{I}\right) = \left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor + 1$, $\left\lfloor \frac{P}{\widetilde{P}} \right\rfloor - 1 \le \left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor \le \left\lfloor \frac{P}{\widetilde{P}} \right\rfloor$, and

$$\left\lfloor \frac{P}{\widetilde{P}} \right\rfloor \le f\left(\widetilde{I}\right) \le \left\lfloor \frac{P}{\widetilde{P}} \right\rfloor + 1. \tag{14}$$

The statement is proven. □

Let us study how the cardinality of the enumeration sets of the Asmuth-Bloom scheme and DT-RRNS are related to RRNS parameters. The Asmuth-Bloom scheme is determined by the set of moduli $p_0 < p_1 < p_2 < \ldots < p_k < p_{k+1} < \ldots < p_n$. To ensure the asymptotic ideality of the Asmuth-Bloom SSS, we require that this sequence be compact with the initial value p_0, or $p_n < p_0 + p_0^\theta$ for $\theta \in (0,1)$. In this case, the sequence $p_1 < \ldots < p_n$ will be compact with the initial value p_1. This RRNS will be used as the basis for the proposed DT-RRNS.

The cardinality of the Asmuth-Bloom enumeration set is constant and equal to p_0.

$$\left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor \le f\left(\widetilde{I}_{max}\right) \le \left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor + 1 < p_0. \tag{15}$$

$\widetilde{I}_{max}$ is a set of unauthorized subsets numbers with the largest range $\widetilde{P}_{max}$, then,

$$\widetilde{P}_{max} = \prod_{i=0}^{k-2} p_{n-i}. \tag{16}$$

Establish a relationship between the value $f\left(\widetilde{I}_{max}\right)$ and k. Let us consider two SSSs with a threshold k and $n-k+1$, assuming $2 \le k \le \frac{n}{2}$.

Let us calculate $\frac{P}{\widetilde{P}_{max}}$ for the second SSS:

$$\frac{\prod_{i=1}^{n-k+1} p_i}{\prod_{i=0}^{n-k-1} p_{n-i}} = \frac{p_1 \cdot p_2 \cdot \ldots \cdot p_k \cdot p_{k+1} \cdot \ldots \cdot p_{n-k+1}}{\cdot p_{k+1} \cdot p_{k+2} \cdot \ldots \cdot p_{n-k+1} \cdot p_{n-k+2} \cdot \ldots \cdot p_n} = \frac{p_1 \cdot p_2 \cdot \ldots \cdot p_k}{p_{n-k+2} \cdot \ldots p_n} = \frac{\prod_{i=1}^{k} p_i}{\prod_{i=0}^{k-2} p_{n-i}}. \tag{17}$$

The expression on the right is the value $\frac{P}{\widetilde{P}_{max}}$ for the first SSS. Therefore, the values $\frac{P}{\widetilde{P}_{max}}$ symmetrical in k regarding the meaning $\lfloor \frac{n}{2} \rfloor$. Let now $2 \leq k < \lfloor \frac{n}{2} \rfloor$ and $k_1 = k+1$. Let now $f_{k_1} = \frac{P}{\widetilde{P}_{max}}$ for a threshold k_1. Let us estimate the value f_{k_1}:

$$f_{k_1} = \frac{\prod_{i=1}^{k_1} p_i}{\prod_{i=0}^{k_1-2} p_{n-i}} = \frac{\prod_{i=1}^{k+1} p_i}{\prod_{i=0}^{k-1} p_{n-i}} = \frac{p_{n-k+2}}{p_{k+1}} \cdot \frac{\prod_{i=1}^{k} p_i}{\prod_{i=0}^{k-2} p_{n-i}} = \frac{p_{n-k+2}}{p_{k+1}} \cdot f_k. \tag{18}$$

where f_k represents the value $\frac{P}{\widetilde{P}_{max}}$ for SSS with threshold k. Because $2 \leq k < \frac{n}{2}$, then, $n-k+2 > \frac{n}{2}$, therefore, $n-k+2 > k+1$. Considering the restrictions imposed on the RRNS moduli, we have $p_{n-k+2} > p_{k+1}$, therefore, $\frac{p_{n-k+2}}{p_{k+1}} > 1$.

Given the above considerations, we obtain that $f_{k_1} < f_k$. In other words, the worst case in which $\frac{P}{\widetilde{P}_{max}}$ takes the smallest value is the case $k = \lfloor \frac{n}{2} \rfloor$. Because of the symmetry $\frac{P}{\widetilde{P}_{max}}$ relative to this value, it is advisable to consider k within the borders $\left[2, \frac{n}{2}\right]$, as for the interval $\left[\frac{n}{2}, n-1\right]$ reasoning proceeds in a similar way. A special case is SSS in which $k = n$ and $\frac{P}{\widetilde{P}_{max}} = 1$.

Next, we prove several important statements that accurately estimate $f\left(\widetilde{I}_{max}\right)$.

Statement 3. *For any sequence $p_1 < p_2 < \ldots < p_n$ follows that*

$$f\left(\widetilde{I}_{max}\right) = \begin{cases} \lfloor \frac{P}{\widetilde{P}_{max}} \rfloor + 1 \text{ if } \widetilde{s} < |P|_{\widetilde{P}_{max}}, \\ \lfloor \frac{P}{\widetilde{P}_{max}} \rfloor, \qquad otherwise \end{cases} \tag{19}$$

Proof. From Statement 2, it follows

$$f\left(\widetilde{I}_{max}\right) = \lfloor \frac{P - \widetilde{s} - 1}{\widetilde{P}} \rfloor + 1. \tag{20}$$

If $\widetilde{s} < |P|_{\widetilde{P}_{max}}$ then $\frac{P-\widetilde{s}-1}{\widetilde{P}} \geq \frac{P-|P|_{\widetilde{P}_{max}}}{\widetilde{P}_{max}} = \left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor$ else $\frac{P-\widetilde{s}-1}{\widetilde{P}} < \frac{P-|P|_{\widetilde{P}_{max}}}{\widetilde{P}_{max}} = \left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor$. Hence if $\widetilde{s} < |P|_{\widetilde{P}_{max}}$ then $\left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor = \left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor$ else $\left\lfloor \frac{P-\widetilde{s}-1}{\widetilde{P}} \right\rfloor = \left\lfloor \frac{P}{\widetilde{P}_{max}} \right\rfloor - 1$.

The statement is proven. □

Expression (20) shows the upper bound for $f(\widetilde{I}_{max})$. To estimate the lower bound $f\left(\widetilde{I}_{max}\right)$, we prove the following statement.

Statement 4. *For any sequence $p_1 < p_2 < \ldots < p_n$ such that $p_n < p_1 + p_1^{\theta}$, $0 < \theta < 1$, and any k such that $2 \leq k < \lfloor \frac{n}{2} \rfloor$, the following inequality is satisfied*

$$f\left(\widetilde{I}_{max}\right) = \frac{P}{\widetilde{P}_{max}} > p_1 \left(\frac{1}{1 + p_1^{\theta-1}} \right)^{k-1}. \tag{21}$$

Proof. Since the sequence is compact with the initial value p_1, then $\widetilde{P}_{max} < \left(p_1 + p_1^{\theta}\right)^{k-1}$. On the other hand, since the sequence is increasing, then $P > p_1^k$. Consequently

$$f\left(\widetilde{I}_{max}\right) = \frac{P}{\widetilde{P}_{max}} > \frac{p_1^k}{\left(p_1 + p_1^{\theta}\right)^{k-1}} = p_1 \left(\frac{p_1}{p_1 + p_1^{\theta}} \right)^{k-1} = p_1 \left(\frac{1}{1 + p_1^{\theta-1}} \right)^{k-1}, \tag{22}$$

from which the inequality (21) follows. The statement is proven. □

Based on Statements 3 and 4, let us accurately determine the boundaries for the quantity $\frac{P}{\widetilde{P}_{max}}$, which directly depends on the value p_1.

Let us consider an example that shows how fast the value $\frac{P}{\widetilde{P}_{max}}$ converges to p_1.

Figure 4 shows $R = \frac{f(\widetilde{I}_{max})}{p_1}$. R shows the relation of $f\left(\widetilde{I}_{max}\right)$ and p_1. This relation assesses how parameter a affects security by approaching the value of b by using compact sequences for various p_1. We see that with increasing p_1, R approaches 1, and, therefore, $\frac{P}{\widetilde{P}_{max}}$ approaches p_1. In this case, Equation (22) estimates the lower bound of R.

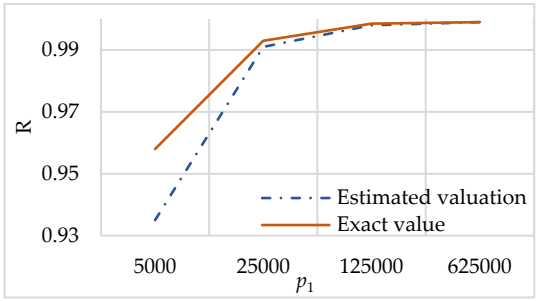

Figure 4. $R = \frac{f(\widetilde{I}_{max})}{p_1}$ varying p_1 for $\theta = 0.477$, $n = 15$, and $k = 7$.

Statement 4 estimates the proximity of the cardinality of possible secrets $f\left(\widetilde{I}_{max}\right)$ to p_1 depending on the p_1, θ, k, and n given before generating the sequence itself.

Figure 4 shows that the higher the value of p_1, the closer $f\left(\widetilde{I}_{max}\right)$ to it. Thus, with a higher value of p_1, the DT-RRNS has higher security.

Statement 4 is important for estimating security. At fixed θ and k, magnitude $f\left(\widetilde{I}_{max}\right) = \frac{P}{\widetilde{P}_{max}}$ is within the following limits:

$$p_1\left(\frac{1}{1+p_1^{\theta-1}}\right)^{k-1} < \frac{P}{\widetilde{P}_{max}} \tag{23}$$

It is easy to show that for fixed $0 < \theta < 1$ and $2 \le k \le n$

$$\lim_{p_1\to\infty}\left(\frac{1}{1+p_1^{\theta-1}}\right)^{k-1} = 1 \text{ and } \frac{1}{1+p_1^{\theta-1}} < 1. \tag{24}$$

Consequently,

$$\left(\frac{1}{1+p_1^{\theta-1}}\right)^{k-1} = (1-\varepsilon), \tag{25}$$

where $0 < \varepsilon < 1$. And the more p_1, the closer ε to 0. Then from (24) it follows

$$p_1(1-\varepsilon) < \frac{P}{\widetilde{P}_{max}}, \tag{26}$$

Based on this expression, one can obtain the following estimate for $f\left(\widetilde{I}_{max}\right)$:

$$p_1 - \varepsilon p_1 < f\left(\widetilde{I}_{max}\right). \tag{27}$$

The last inequality determines the degree of closeness of the quantity $f\left(\widetilde{I}_{max}\right)$ to p_1 without generating the sequence itself. Because $p_1 > p_0$ then due to restrictions imposed

on $\frac{P}{\widetilde{P}_{max}}$, with an increasing number p_0, the cardinality $f\left(\widetilde{I}_{max}\right)$ of the enumeration set of DT-RRNS approaches p_1. We can conclude that the cardinality of the brute force set for the DT-RRNS when choosing sufficiently large moduli is equivalent to the cardinality of the brute force set of the Asmuth-Bloom scheme, which is equal to p_0.

Let us now compare the DT-RRNS with the Mignotte scheme. The basic design requirement of the Mignotte scheme is the inclusion of a secret s into the interval $\left(\alpha = \prod_{i=0}^{k-2} p_{n-i}, \beta = \prod_{i=1}^{k} p_i\right)$. The statements proved earlier regarding the size of the set of enumerations of the DT-RRNS allow us to deviate from this rule in favor of increasing the dynamic range of the secret representation. Based on the assumption of a uniform distribution of the secret in the interval $[0, P)$, compactness of the set $p_0 < p_1 < \ldots < p_n$ and a sufficiently large number p_0, it is easy to show that the probability of a secret falling into the interval $[0, \alpha)$ approaches the probability of "guessing" an arbitrary secret in the Asmuth-Bloom scheme.

Note that in the notation used, $\alpha = \widetilde{P}_{max}$ and $\beta = P$. Indeed, the secret in the Asmuth-Bloom scheme is in the range $\left[0, \mathrm{p}_0\right)$ and is determined by p_0. With a uniform distribution of the secret on this set, the probability of choosing an arbitrary secret is $\frac{1}{p_0}$. On the other hand, the probability of a number falling into the interval $[0, \alpha) = \left[0, \widetilde{P}_{max}\right)$ is equal to $\frac{|[0, \widetilde{P}_{max})|}{|[0,P)|\frac{\widetilde{P}_{max}}{P}}$. According to Statement 3, for a sufficiently large p_0, the magnitude $\frac{P}{\widetilde{P}_{max}}$ is equivalent to p_0.

It follows that parameters that are determined by DT-RRNS can eliminate restrictions imposed on the parameters of the Mignotte scheme. Let us consider examples of generating DT-RRNS parameters.

Example 1. *Let* $p_1 = 1024$, $n = 10$, *and* $k = 5$, *and let it be required that the deviation from the Asmuth-Bloom search power does not exceed 10%. Determine what should be* θ *in this case. According to estimates (24) and (28), we obtain*:

$$\theta < \log_{p_1}\left(\frac{1}{\sqrt[k-1]{1-\varepsilon}} - 1\right) + 1, \tag{28}$$

whereε*is a required deviation. In our case,*$\varepsilon = 0.05$.

Substituting the available data into the formula, we have $\theta < 0.477$.

Consequently, the numbers that provide the required cardinality of the enumeration set must be within the interval $[1024, 1051)$. *Using Statement 4, we have*

$$f\left(\widetilde{I}_{max}\right) > p_1\left(\frac{1}{1+p_1^{\theta-1}}\right)^{k-1} = 1024\left(\frac{1}{1+1024^{0.477-1}}\right)^4 \approx 921.762.$$

Fewer unique divisors of p_1, the more beneficial to use them for building a compact sequence. It increases the number of the coprime numbers in the interval from p_1 to $2p_1$.

It is worth noting that the proof of the possibility of generating compact sequences is a difficult number-theoretic problem.

The generation of a variety of compact sequences is the subject of further research. Now, we can limit ourselves to practical recommendations, which consist in choosing sufficiently large p_1 and with the least number of divisors.

Statements 1–4 evaluate the security of the DT-RRNS scheme. First, according to Statement 1, $p_1 > 2^{k-1}$ determines a lower bound of p_1. For maximum security, p_1 must be significantly higher than 2^{k-1}. Secondly, an important parameter of the scheme is the value θ, defining a compact sequence. The closer θ to zero, the better the SSS properties in terms of security, which follows from Statement 4 and inequality (24).

7. Security of Data Transmission

The RRNS allows the implementation of the integrity, availability, and confidentiality of data by a single mechanism. These features provide an efficient way to ensure reliability and security during data transmission in MANET.

This section discusses the principles on which the proposed method of data transmission in a non-hierarchical network is based.

To meet MANET requirements, we choose a symmetric encryption scheme, a secure RRNS with a compact set of moduli $\{p_1, p_2, \ldots, p_k, p_{k+1}, \ldots, p_n\}$, for which $p_n < p_1 + p_1^{\theta}$, where $0 < \theta < 1$. To provide the required level of security, the moduli must be close in size to each other.

The combined use of multipath routing, a secure sharing scheme, and the error correction capabilities of RRNS create the conditions for using a new approach to data transport that guarantees transmission reliability and security.

The main principles of the proposed approach:

1. Data are encrypted by a symmetric encryption algorithm and key K.
2. The encrypted data are represented as a set of n RRNS shares by dividing it on moduli $\{p_1, p_2, \ldots p_k, p_{k+1}, \ldots, p_n\}$.
3. Key K is divided based on the perfect Asmuth-Bloom scheme to guarantee a high level of key security.
4. Shares of the secret, which consist of a share of the key and data shares, are sent by a separate route that is associated with this modulo and obtained according to an algorithm with the possibility of multipath routing with division by nodes.
5. If some of them could not be delivered within the given waiting period, the receiving node carries out a verification procedure, which is based on the ability of the RRNS to correct and control data integrity.
6. After checking secret shares for correctness and integrity, the receiving node performs a recovery procedure.
7. To recover the original data, the receiver needs to recover the secret key from key shares and decrypt the data using the obtained key.

Figure 5 shows a generalized scheme of the proposed method of data transmission based on encryption, encoding, and data sharing using RRNS. The key is generated first since its size affects the redundancy of the scheme and, therefore, the overall network load.

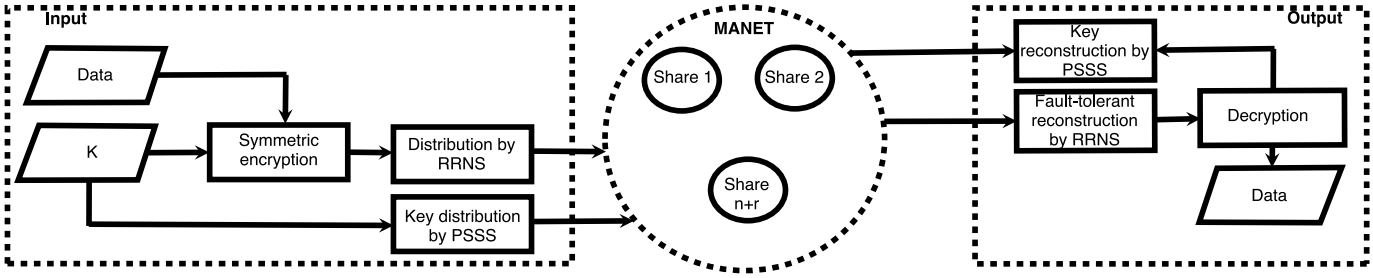

Figure 5. A generalized scheme for secure and reliable data transmission based on a computationally secure SSS.

Shares are moved along one of the previously constructed routes without crossing the nodes. After receiving all or part of the shares of the secret, the receiver recovers the secret by performing the error-correcting decoding procedure. The original secret is obtained by decrypting the data decoded from the RRNS using the encryption key.

To balance the network load, a weighted SSS is used [39]. The route weight, route length, and route reliability (if a secure routing algorithm is used) can be adapted by changing RRNS parameters.

For example, the shortest route can be associated with the largest RRNS modulo. In this case, the message of this route will be the largest, but the transmission along it will be

faster. By associating moduli with routes, we can achieve an increase in the quality and speed of transmission and an overall offload of the data transmission network.

The share of the secret that is represented by the smallest modulo carries less information about the original secret relative to the information by the larger modulo. This feature is applicable to change the flow of information to increase the security of data transmission, transporting the smallest share of the secret along the least reliable route according to some criterion.

The proposed approach is characterized by a combination of reliability and security, which are achieved due to several factors. Reliability is based on multipath routing and the RRNS error correction code.

The reliability of a set of routes W depends on the reliability of all constructed routes as follows [3]:

$$1 - \prod_{\omega \in W} \left(1 - \Pi_{S,D}^{\omega}(t)\right), \tag{29}$$

where $\Pi_{S,D}^{\omega}(t) = \prod_{\{a,b\} \in \omega} A_{a,b}(t)$—reliability of a single route $\omega \in W$, which is the product of the availability $A_{a,b}$ of each of the connections between the nodes a and b at a certain point in time t.

We see that with an increase in the number of routes, the reliability of data transmission increases. In addition, RRNS increases the reliability of data transmission due to excessive noise-resistant coding. RRNS controls not only the situation with the loss of availability of an individual node and connectivity but also damage due to failures and intentional distortion of information.

8. Security Analysis

Now, let us consider the security of data transmission through MANET by the proposed method. As noted earlier, security is based on the strength of the RRNS-SSS. The computationally secure SSS has a sufficient level of security without leading to high redundancy, unlike ideal SSSs [39]. Due to the properties of RRNS, this scheme allows not only secure data transmission in networks but also load balancing using distributed transmission of data divided into small shares.

The strength of a particular network configuration depends on the resistance of each node to capture, the network topology, the number of node-separated routes built, the configuration of the SSS, and the moduli selection of the RRNS. It is necessary to consider that the condition for data interception (and at the same time confidentiality violation) is the interception of any number of nodes on n or more routes. Because it is not known in advance which nodes will be intercepted, it is impossible to select and exclude a compromised route in the data transmission protocol.

Let us introduce the following notations:

Pr—the probability of secure data transmission when data will not be intercepted during the time interval T_0.
Pr_{node}—the probability of the node attack-resistance (the probability that during the time interval T_0 the data on the node will not be intercepted).
Q_z—the probability of interception of z nodes.
E_z—the probability of secret loss with z intercepted nodes.
Pr_z—the probability of secure data transmission with z intercepted nodes
$node_{ij}$,—node j in the route i.
Z—the total number of nodes.
z—number of intercepted nodes.

Let us consider the probability Pr for the example of the network with the same number of nodes on each route. Note, that it can be extended to the case with an arbitrary number of nodes on each route.

Let us have four possible data transmission routes (Figure 6), each of which has two nodes, with $\Pr_{\text{node}} = 0.99$. We use a suitable RRNS configuration $(3, 4)$ with three working and one redundant modulo.

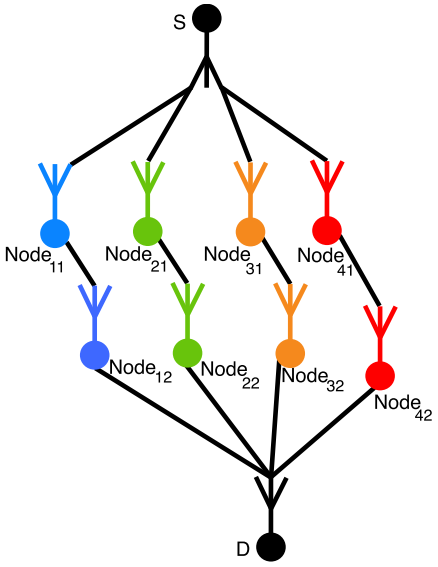

Figure 6. Routing example for 4 non-crossing routes with 2 nodes per each route.

The probability of interception is 1–Pr. The interception of data at any of the nodes of the route means the loss of confidentiality of the data transmitted by this route.

To intercept the secret, at least three different routes must be intercepted (according to the number of moduli $k = 3$, the minimum necessary for recovery). Therefore, the probability of interception when less than three nodes are intercepted is zero.

If exactly three nodes are attacked, then there are two options:

- An attacker will be able to recover the original message, for example, if nodes are node_{11}, node_{21}, node_{42};
- An attacker will not be able to recover the original message, for example, if nodes are node_{11}, node_{12}, node_{22}.

The number of possible permutations of 8 nodes taken 3 intercepted at a time that leads to loss of secret (we denote this value by E_3), multiplied by the probability of intercepting exactly three nodes, gives the probability $\Pr_3$ of intercepting data when intercepting any three nodes:

$$\Pr_3 = Q_3 E_3, \tag{30}$$

where $Q_3 = (1 - \Pr_{\text{node}})^3 \Pr_{\text{node}}^5$—the probability of intercepting exactly three nodes.

In general, the probability Q_z of interception z nodes are calculated considering the formula:

$$Q_z = (1 - \Pr_{\text{node}})^z \Pr_{\text{node}}^{Z-z}. \tag{31}$$

For example, if $E_3 = 32$, then

$$\Pr_3 = 32 \cdot (1 - 0.99)^3 \cdot 0.99^5 = 0.0000304316816$$

If exactly four nodes were intercepted, then there are also two options:

- An attacker will be able to recover the original data, for example, if the intercepted nodes are node_{11}, node_{12}, node_{21}, node_{42};
- The attacker will not be able to recover the original data, for example, if the intercepted nodes are node_{11}, node_{12}, node_{21}, node_{22}.

The number of combinations E_4 of the four captured nodes, allowing you to recover the original data, multiplied by the probability of intercepting exactly four nodes, will give the probability of intercepting data if any four nodes are intercepted:

$$\Pr_4 = Q_4 E_4 \tag{32}$$

For example, if $E_4 = 64$ then $\Pr_4 = 6.147814464 \times 10^{-7}$.

Special attention deserves the case if five or more nodes are intercepted. In the described situation, any set of captured nodes will provide attackers with a means to recover the original data. For situations of this kind, the number of combinations of received nodes that are needed to recover the original message will be equal to the total number of permutations with repetitions of 8 nodes of 5, 6, 7, and 8, respectively. Calculated values: $E_5 = 56$, $E_6 = 28$, $E_7 = 8$, $E_8 = 1$, Then, guided by the approach proposed earlier, we obtain that $Pr_5 = 5.434 \times 10^{-9}$, $Pr_6 = 2.744 \times 10^{-11}$, $Pr_7 = 7.92 \times 10^{-14}$ и $Pr_8 = 10^{-16}$.

Using the results of probability calculations for each of the cases, it is possible to isolate the overall probability of intercepting data:

$$1 - Pr = \sum_{z=3}^{8} Pr_z = 0.000031052$$

It turns out that the probability Pr of secure data transmission is $Pr = 0.999968948$ for $\Pr_{\text{node}} = 0.99$.

Table 1 shows the probability Pr of secure data transmission in MANET with redundant (3,4)-RRNS four possible data transmission routes and two nodes on each of the routes, for different values of Pr_{node}.

Table 1. Probability of secure data transmission Pr_z with z intercepted nodes for the different probability of the node attack resistance.

z	Pr_{node} = 0.7		Pr_{node} = 0.9		Pr_{node} = 0.99	
	Pr_z	Q_z	$\Pr_z$	Q_z	$\Pr_z$	Q_z
0	1	5.757×10^{-2}	1	4.304×10^{-1}	1	9.22×10^{-1}
1	1	2.47×10^{-2}	1	4.782×10^{-2}	1	9.32×10^{-3}
2	1	1.05×10^{-2}	1	5.314×10^{-3}	1	9.4×10^{-5}
3	1.452×10^{-1}	4.537×10^{-3}	1.88×10^{-4}	5.9×10^{-4}	3.04×10^{-5}	9.509×10^{-7}
4	1.244×10^{-1}	1.944×10^{-3}	4.199×10^{-4}	6.5×10^{-5}	6.147×10^{-7}	9.605×10^{-9}
5	4.667×10^{-2}	8.33×10^{-3}	4.08×10^{-4}	7×10^{-6}	5.433×10^{-9}	9.702×10^{-11}
6	10^{-2}	3.57×10^{-4}	2.2×10^{-5}	8.1×10^{-7}	2.744×10^{-11}	9.801×10^{-13}
7	1.224×10^{-3}	1.53×10^{-4}	7.2×10^{-7}	9×10^{-8}	7.92×10^{-14}	9.9×10^{-15}
8	6.56×10^{-3}	6.5×10^{-5}	10^{-8}	10^{-8}	10^{-16}	10^{-16}
	$Pr = 6.723 \times 10^{-1}$		$Pr = 9.764 \times 10^{-1}$		$Pr = 9.999 \times 10^{-1}$	

Table 1 shows that for $z = 0, 1, 2$ the probability Q_z is high. However, data transmitted by DT-RRNS are not intercepted. If $z \geq 3$ and $\Pr_{\text{node}} \geq 0.7$, probability $Q_z \leq 4.537 \times 10^{-3}$, which reduces the probability of secure data transmission $\Pr_z$.

We note that with increasing the number of possible routes and corresponding changing RRNS parameters, the probability of a secure data transmission increases.

Table 2 shows that the probability of a secure transmission grows quite fast with increasing (k, n) parameters and number of nodes, even for the high probability of the resistance of the node to data interception $\Pr_{\text{node}} = 0.99$.

Table 2. Probability *Pr* of secure data transmission at different numbers of routes and the total number of nodes.

(*k*, *n*)/Number of Nodes	**Pr**	
	Pr_{node} = 0.9	**Pr_{node} = 0.99**
(2, 3)/6	0.905	0.998827731
(3, 4)/8	0.976	0.999968948
(4, 5)/10	0.994	0.999999228
(5, 6)/12	0.998	0.999999982
(6, 7)/14	0.9997	0.999999999
(7, 8)/16	0.9999	0.999999999

9. Performance Analysis

In this section, we compare two SSS-RRNS solutions: well-known Asmuth-Bloom and DT-RRNS. To measure encoding time, decoding time, and redundancy, we transmit data from 6 MB to 146 MB across a network of 16–24 nodes with 4 neighboring nodes, using a number of moduli from 4 to 6. The secret key used for the schemes is 2147483659.

Table 3 and Figure 7 show the encoding and decoding time, and redundancy for the Asmuth-Bloom and DT-RRNS schemes with varying data sizes and the number of moduli. We see that the encoding and decoding times increase linearly for both Asmuth-Bloom and DT-RRNS.

Table 3. The coding and decoding time and redundancy.

Scheme	Moduli	Data Size (KB)	Coding Time (ms)	Redundancy	Decoding Time (ms)
Asmuth-Bloom	4	6076	52	5.33772	57
DT-RRNS			9	1.07176	12
Asmuth-Bloom		23,974	129	5.33445	136
DT-RRNS			27	1.06782	32
Asmuth-Bloom		98,927	519	5.33355	494
DT-RRNS			107	1.06697	116
Asmuth-Bloom		103,673	547	5.33354	523
DT-RRNS			113	1.06689	119
Asmuth-Bloom		111,108	589	5.33348	560
DT-RRNS			120	1.06693	127
Asmuth-Bloom		137,016	719	5.33345	676
DT-RRNS			148	1.06685	156
Asmuth-Bloom		146,133	776	5.33344	719
DT-RRNS			158	1.06686	165
Asmuth-Bloom	5	6076	44	6.67215	58
DT-RRNS			9	1.05662	12
Asmuth-Bloom		23,974	158	6.66806	166
DT-RRNS			26	1.05364	29
Asmuth-Bloom		98,927	632	6.66694	593
DT-RRNS			102	1.0529	117
Asmuth-Bloom		103,673	662	6.66692	614
DT-RRNS			107	1.05293	119
Asmuth-Bloom		111,108	708	6.66685	668
DT-RRNS			115	1.05285	129
Asmuth-Bloom		137,016	872	6.66681	809
DT-RRNS			142	1.05287	151
Asmuth-Bloom		146,133	930	6.6668	866
DT-RRNS			152	1.05288	165

Table 3. *Cont.*

Scheme	Moduli	Data Size (KB)	Coding Time (ms)	Redundancy	Decoding Time (ms)
Asmuth-Bloom	6	6076	56	8.00658	69
DT-RRNS			8	1.05069	11
Asmuth-Bloom		23,974	186	8.00167	187
DT-RRNS			26	1.04513	32
Asmuth-Bloom		98,927	740	8.00032	693
DT-RRNS			102	1.04392	114
Asmuth-Bloom		103,673	778	8.00031	720
DT-RRNS			106	1.04382	122
Asmuth-Bloom		111,108	829	8.00022	772
DT-RRNS			112	1.04374	125
Asmuth-Bloom		137,016	1026	8.00018	944
DT-RRNS			139	1.04379	152
Asmuth-Bloom		146,133	1097	8.00016	1011
DT-RRNS			148	1.04371	160

DT-RRNS shows better runtime results than Asmuth-Bloom. DT-RNS for the largest data size has less time than Asmuth-Bloom for the smallest data size when using 6 moduli. The redundancy for DT-RRNS is approximately the same for all moduli sets and data sizes. The redundancy of the Asmuth-Bloom is increasing with the number of moduli increasing.

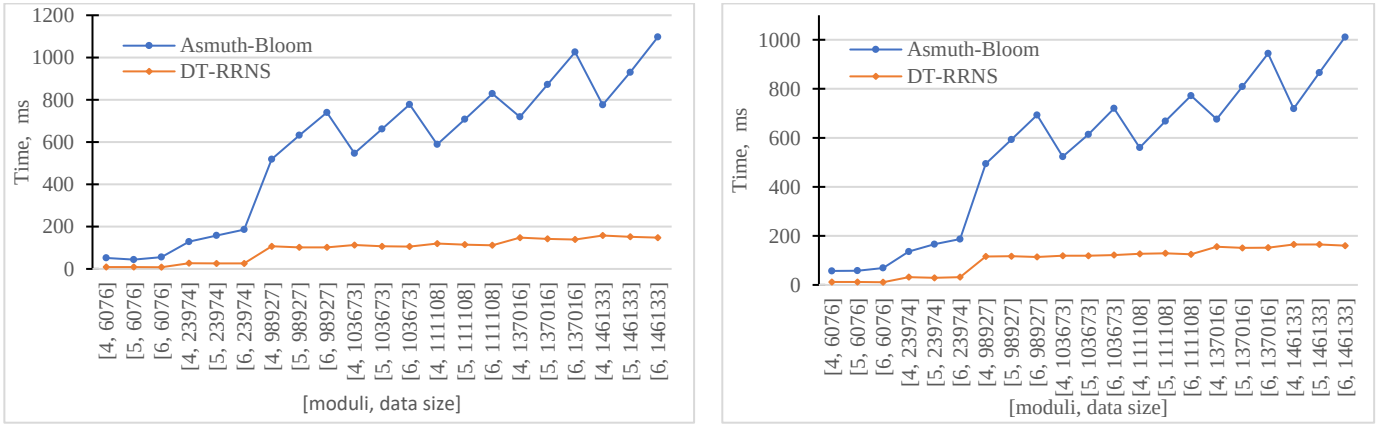

Figure 7. Encoding time and obtained redundancy for Asmuth-Bloom and DT-RRNS (**a**) Encoding time. (**b**) Decoding time.

Table 4 contains the moduli used in the experiment.

Table 4. Number of moduli and their meanings.

Number of Moduli	Moduli
4	(2147483693, 2147483713, 2147483743, 2147483777)
5	(2147483693, 2147483713, 2147483743, 2147483777, 2147483783)
6	(2147483693, 2147483713, 2147483743, 2147483777, 2147483783, 2147483813)

Figure 7 shows the encoding time (a) and decoding time (b) versus the number of moduli and data size. Figure 8 shows the redundancy versus the number of moduli and data size. DT-RRNS has lower redundancy close to 1. We see that the redundancy of both Asmuth-Bloom and DT-RRNS weakly depends on the input data. It varies with scheme parameters.

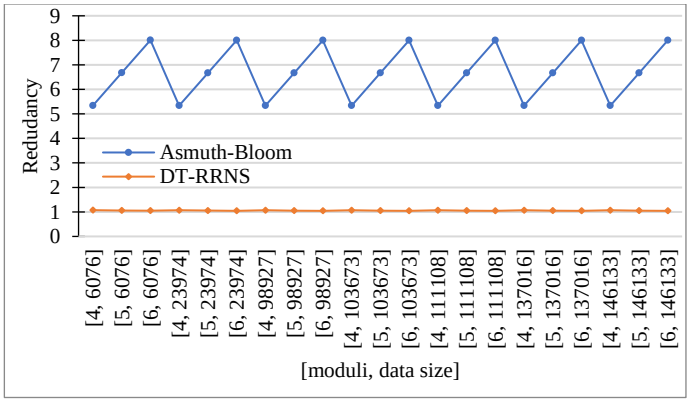

Figure 8. Redundancy.

We see that the proposed DT-RRNS has several advantages. It increases the speed of the system. The encoding time is in the range of 1 to 180 ms, while Asmuth-Bloom is between 40 and 1100 ms. It has reduced data redundancy while maintaining the same level of security and reliability.

10. Concluding Discussion

Large-scale data sharing in a distributed smart city environment requires an increased attention to data security and reliability issues. Methods that ensure data security at the required level with high reliability and speed are very important.

In this work, we propose a DT-RRNS routing solution for the WSN and MANET complex dynamic hierarchical heterogeneous networks for improving data transmission. To design efficient mechanisms, we consider reliability and security as close concepts. Increased security and reliability are achieved with an effective data recovery mechanism of RRNS with moduli of compact sequences of coprime numbers.

This mechanism together with adaptive multipath routing increases the resistance of the sensor network to attacks of various types, including unauthorized interception, message falsification, errors, node and network connection failures, information loss in case of attacks or accidents, etc.

This approach does not have the limitations of the traditional encryption methods for secured data transmission. The secret key management is solved by the SSS.

In addition, this solution reduces data redundancy, resulting in less use of large equipment, energy consumption, and message storage capacity. These properties are important when deploying IoT.

In the DT-RRNS, each participant receives shares of a smaller size than the original data. It improves transmission speed, resulting in better support for big data sensing and processing, in contrast to the Asmuth-Bloom scheme.

The promising direction for future work is the development of computationally efficient methods for generating dynamic RRNS parameters and dynamic routes due to loss of sensors, connections, loss of functionality, errors by contamination, vibration, shocks, high temperatures, etc. It is important to study the problem of selecting moduli for dynamic adaptation to changing network topology and characteristics. To further improve efficiency and reliability, we will consider specialized multipath routing protocols based on a weighted version of DT-RRNS.

Author Contributions: A.G.: conceptualization, methodology, software, validation, research, writing; E.S.: conceptualization, methodology, software, validation, research, writing; A.T.: conceptualization, methodology, research, writing, supervision; M.D.: methodology, research, writing; M.B.: conceptualization, methodology, research, writing, supervision; S.N.: conceptualization, methodology, research, writing. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Ministry of Education and Science of the Russian Federation (Project 075-15-2020-788).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Deakin, M.; Al Waer, H. From Intelligent to Smart Cities. *Intell. Build. Int.* **2011**, *3*, 140–152. [CrossRef]
2. Weinstein, R. RFID: A Technical Overview and Its Application to the Enterprise. *IT Prof.* **2005**, *7*, 27–33. [CrossRef]
3. Zahid, S.; Ullah, K.; Waheed, A.; Basar, S.; Zareei, M.; Biswal, R.R. Fault Tolerant DHT-Based Routing in MANET. *Sensors* **2022**, *22*, 4280. [CrossRef] [PubMed]
4. Skokowski, P.; Malon, K.; Lopatka, J. Building the Electromagnetic Situation Awareness in MANET Cognitive Radio Networks for Urban Areas. *Sensors* **2022**, *22*, 716. [CrossRef] [PubMed]
5. Chiejina, E.; Xiao, H.; Christianson, B.; Mylonas, A.; Chiejina, C. A Robust Dirichlet Reputation and Trust Evaluation of Nodes in Mobile Ad Hoc Networks. *Sensors* **2022**, *22*, 571. [CrossRef]
6. Gladkov, A.; Shiriaev, E.; Tchernykh, A.; Deryabin, M.; Bezuglova, E.; Valuev, G.; Babenko, M.; Nesmachnow, S. SNS-Based Secret Sharing Scheme for Security of Smart City Communication Systems. In *Communications in Computer and Information Science, CCIS, Proceedings of Smart Cities. ICSC-CITIES 2022*; Nesmachnow, S., Hernández Callejo, L., Eds.; Springer: Cham, Switzerland, 2023; Volume 1706, pp. 248–263. [CrossRef]
7. Weissman, J.B. Gallop: The Benefits of Wide-Area Computing for Parallel Processing. *J. Parallel. Distrib. Comput.* **1998**, *54*, 183–205. [CrossRef]
8. Lange, D.B. Mobile Objects and Mobile Agents: The Future of Distributed Computing? In *ECOOP'98—Object-Oriented Programming*; Jul, E., Ed.; Springer: Berlin/Heidelberg, Germany, 1998; pp. 1–12.
9. Datla, D.; Chen, X.; Tsou, T.; Raghunandan, S.; Hasan, S.M.S.; Reed, J.H.; Dietrich, C.B.; Bose, T.; Fette, B.; Kim, J.-H. Wireless Distributed Computing: A Survey of Research Challenges. *IEEE Commun. Mag.* **2012**, *50*, 144–152. [CrossRef]
10. Lobo, P.; Acharya, S.; D'Souza, R.O. Quality Of Service For Manet Based Smart Cities. *Int. J. Adv. Comput. Eng. Netw.* **2017**, *5*, 6.
11. Cardone, G.; Bellavista, P.; Corradi, A.; Foschini, L. Effective Collaborative Monitoring in Smart Cities: Converging MANET and WSN for Fast Data Collection. In Proceedings of the ITU Kaleidoscope 2011: The Fully Networked Human?—Innovations for Future Networks and Services (K-2011), Cape Town, South Africa, 12–14 December 2011; pp. 1–8.
12. Pandey, J.; Kush, A.; Dattana, V.; Ababseh, R.A. Novel Scheme to Heal MANET in Smart City Network. In Proceedings of the 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 15–16 March 2016; pp. 1–6.
13. Shiryaev, E.; Bezuglova, E.; Babenko, M.; Tchernykh, A.; Pulido-Gaytan, B.; Cortés-Mendoza, J.M. Performance Impact of Error Correction Codes in RRNS with Returning Methods and Base Extension. In Proceedings of the 2021 International Conference Engineering and Telecommunication (En&T), Dolgoprudny, Russia, 24–25 November 2021; pp. 1–5.
14. Babenko, M.; Nazarov, A.; Tchernykh, A.; Pulido-Gaytan, B.; Cortés-Mendoza, J.M.; Vashchenko, I. Algorithm for Constructing Modular Projections for Correcting Multiple Errors Based on a Redundant Residue Number System Using Maximum Likelihood Decoding. *Program Comput. Soft* **2021**, *47*, 839–848. [CrossRef]
15. Babenko, M.; Tchernykh, A.; Pulido-Gaytan, B.; Cortés-Mendoza, J.M.; Shiryaev, E.; Golimblevskaia, E.; Avetisyan, A.; Nesmachnow, S. RRNS Base Extension Error-Correcting Code for Performance Optimization of Scalable Reliable Distributed Cloud Data Storage. In Proceedings of the 2021 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Portland, OR, USA, 17–21 June 2021; pp. 548–553.
16. Tay, T.F.; Chang, C.-H. A New Algorithm for Single Residue Digit Error Correction in Redundant Residue Number System. In Proceedings of the 2014 IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne, Australia, 1–5 June 2014; pp. 1748–1751.
17. Nachiappan, R.; Javadi, B.; Calheiros, R.N.; Matawie, K.M. Cloud Storage Reliability for Big Data Applications: A State of the Art Survey. *J. Netw. Comput. Appl.* **2017**, *97*, 35–47. [CrossRef]
18. Chang, F.; Dean, J.; Ghemawat, S.; Hsieh, W.C.; Wallach, D.A.; Burrows, M.; Chandra, T.; Fikes, A.; Gruber, R.E. Bigtable: A Distributed Storage System for Structured Data. *ACM Trans. Comput. Syst. (TOCS)* **2008**, *26*, 1–26. [CrossRef]
19. Dimakis, A.G.; Godfrey, P.B.; Wu, Y.; Wainwright, M.J.; Ramchandran, K. Network Coding for Distributed Storage Systems. *IEEE Trans. Inf. Theory* **2010**, *56*, 4539–4551. [CrossRef]
20. Lin, S.-J.; Chung, W.-H.; Han, Y.S. Novel Polynomial Basis and Its Application to Reed-Solomon Erasure Codes. In Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science, Philadelphia, PA, USA, 18–21 October 2014; IEEE: New York, NY, USA; pp. 316–325.
21. Ye, R.; Boukerche, A.; Wang, H.; Zhou, X.; Yan, B. RESIDENT: A Reliable Residue Number System-Based Data Transmission Mechanism for Wireless Sensor Networks. *Wirel. Netw.* **2018**, *24*, 597–610. [CrossRef]

22. Stergiou, C.; Psannis, K.E.; Kim, B.-G.; Gupta, B. Secure Integration of IoT and Cloud Computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [CrossRef]
23. Lee, B.-H.; Dewi, E.K.; Wajdi, M.F. Data Security in Cloud Computing Using AES under HEROKU Cloud. In Proceedings of the 2018 27th Wireless and Optical Communication Conference (WOCC), Taiwan, 30 April–1 May 2018; IEEE: New York, NY, USA; pp. 1–5.
24. Zhou, S.; Du, R.; Chen, J.; He, D.; Deng, H. ESDR: An Efficient and Secure Data Repairing Paradigm in Cloud Storage. *Secur. Commun. Netw.* **2016**, *9*, 3646–3657. [CrossRef]
25. Lin, H.-Y.; Tzeng, W.-G. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *23*, 995–1003.
26. Tchernykh, A.; Babenko, M.; Chervyakov, N.; Miranda-López, V.; Kuchukov, V.; Cortés-Mendoza, J.M.; Deryabin, M.; Kucherov, N.; Radchenko, G.; Avetisyan, A. AC-RRNS: Anti-Collusion Secured Data Sharing Scheme for Cloud Storage. *Int. J. Approx. Reason* **2018**, *102*, 60–73. [CrossRef]
27. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
28. Chervyakov, N.; Babenko, M.; Tchernykh, A.; Kucherov, N.; Miranda-López, V.; Cortés-Mendoza, J.M. AR-RRNS: Configurable Reliable Distributed Data Storage Systems for Internet of Things to Ensure Security. *Future Gener. Comput. Syst.* **2019**, *92*, 1080–1092. [CrossRef]
29. Celesti, A.; Fazio, M.; Villari, M.; Puliafito, A. Adding Long-Term Availability, Obfuscation, and Encryption to Multi-Cloud Storage Systems. *J. Netw. Comput. Appl.* **2016**, *59*, 208–218. [CrossRef]
30. Shen, P.; Liu, W.; Wu, Z.; Xiao, M.; Xu, Q. SpyStorage: A Highly Reliable Multi-Cloud Storage with Secure and Anonymous Data Sharing. In Proceedings of the 2017 International Conference on Networking, Architecture, and Storage (NAS), Shenzhen, China, 7–9 August 2017; IEEE: New York, NY, USA; pp. 1–6.
31. Ali, M.; Bilal, K.; Khan, S.U.; Veeravalli, B.; Li, K.; Zomaya, A.Y. DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security. *IEEE Trans. Cloud Comput.* **2015**, *6*, 303–315. [CrossRef]
32. Gentry, C. Computing Arbitrary Functions of Encrypted Data. *Commun. ACM* **2010**, *53*, 97–105. [CrossRef]
33. Gomathisankaran, M.; Tyagi, A.; Namuduri, K. HORNS: A Homomorphic Encryption Scheme for Cloud Computing Using Residue Number System. In Proceedings of the 2011 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011; IEEE: New York, NY, USA; pp. 1–5.
34. Asmuth, C.; Bloom, J. A Modular Approach to Key Safeguarding. *IEEE Trans. Inf. Theory* **1983**, *29*, 208–210. [CrossRef]
35. Mignotte, M. How to Share a Secret. In Proceedings of the Workshop on Cryptography, Delhi, India, 22–24 December 1982; Springer: Berlin/Heidelberg, Germany, 1982; pp. 371–375.
36. Miranda-López, V.; Tchernykh, A.; Cortés-Mendoza, J.M.; Babenko, M.; Radchenko, G.; Nesmachnow, S.; Du, Z. Experimental Analysis of Secret Sharing Schemes for Cloud Storage Based on Rns. In Proceedings of the Latin American High Performance Computing Conference, Buenos Aires, Argentina, 20–22 September 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 370–383.
37. Krawczyk, H. Secret Sharing Made Short. In Proceedings of the Advances in Cryptology—CRYPTO' 93, Santa Barbara, CA, USA, 22–26 August 1994; Stinson, D.R., Ed.; Springer: Berlin/Heidelberg, Germany; pp. 136–146.
38. Barzu, M.; Ţiplea, F.L.; Drăgan, C.C. Compact Sequences of Co-Primes and Their Applications to the Security of CRT-Based Threshold Schemes. *Inf. Sci.* **2013**, *240*, 161–172. [CrossRef]
39. Quisquater, M.; Preneel, B.; Vandewalle, J. On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem. In Proceedings of the International Workshop on Public Key Cryptography, Paris, France, 12–14 February 2022; Springer: Berlin/Heidelberg, Germany, 2022; pp. 199–210.