

A novel smart multilevel security approach for secure data outsourcing in crisis

Akram Y. Sarhan ^{Corresp. 1}

¹ Department of Information Technology, College of Computing and Information Technology, University of Jeddah, Jeddah, Mecca Province, Saudi Arabia

Corresponding Author: Akram Y. Sarhan
Email address: asarhan@uj.edu.sa

The Interconnected Network or the Internet has revolutionized digital communications. It has expanded worldwide over the past four decades due to numerous features such as connectivity, transparency, hierarchy, and openness. On the other hand, several drawbacks, including mobility, scalability, controllability, security, etc., have been presented due to continuous developments. Although several network paradigms exist to address such disadvantages, many issues remain open. This research proposes a future network paradigm that addresses multilevel security shortcomings. In this research, we contribute the following: (i) proposes a two-routers network-based cyber security architecture for multilevel data sharing; (ii) uses a scheduler to deal with the multilevel transmitted packets scheduling problem; (iii) proposes five algorithms for the studied difficult problem; and (iv) provides an experimental result to show the optimal results obtained by the developed algorithms and compare it with algorithms in the literature. The experimental result shows that the Random-Grouped Classification with Shortest Scheduling Algorithm (RGS) performed the best at 37.7% with a gap of 0.03. This result shows the practicality of our approach in terms of two-machines scheduling problems.

A Novel Smart Multilevel Security Approach for Secure Data Outsourcing in Crisis

Akram Y. Sarhan

Department of Information Technology, College of Computing and Information Technology, University of Jeddah, Jeddah, Saudi Arabia

Abstract

The Interconnected Network or the Internet has revolutionized digital communications. It has expanded worldwide over the past four decades due to numerous features such as connectivity, transparency, hierarchy, and openness. On the other hand, several drawbacks, including mobility, scalability, controllability, security, etc., have been presented due to continuous developments. Although several network paradigms exist to address such disadvantages, many issues remain open. This research proposes a future network paradigm that addresses multilevel security shortcomings. In this research, we contribute the following: (i) proposes a two-routers network-based cyber security architecture for multilevel data sharing; (ii) uses a scheduler to deal with the multilevel transmitted packets scheduling problem; (iii) proposes five algorithms for the studied difficult problem; and (iv) provides an experimental result to show the optimal results obtained by the developed algorithms and compare it with algorithms in the literature. The experimental result shows that the Random-Grouped Classification with Shortest Scheduling Algorithm (RGS) performed the best at 37.7% with a gap of 0.03. This result shows the practicality of our approach in terms of two-machines scheduling problems.

Introduction

Anonymous data outsourcing during a crisis has become a challenge due to numerous reasons presented as follows: (i) the daily amount of data produced and exchanged on the Internet; (ii) the ethical and unethical surveillance; (iii) the complexity of internetworking management; and

(iv) the broken protocol designs and architectures. Nowadays, our world has become data-driven due to several factors. The first factor is the digitization in society and economy and the advances in disruptive technologies, including unmanned aerial vehicle (UAV), artificial intelligence (AI), big data, the Internet of Things (IoT), blockchain, and robots (Al-Gburi et al., 2022; Ali et al., 2022). The second is the diversity of technological platforms and social services, such as YouTube, Google, Facebook, Cloud computing, and Mobile devices. Such services and technologies have produced enormous volumes of Internet traffic that enable information exchange and inspire the world to become data-driven (Luo, 2022; Casado et al., 2006).

However, the endless increase in information accessibility has become a challenge bringing several issues concerning the data, such as analysis, transmission, security, and privacy. Moreover, the imperfections of the existing Internet protocol (IP) network architecture make it difficult to address all issues related to any data-driven model. Scalability, Security, Energy-saving, Quality of Service, and Mobility are the significant issues inherited in the IP network architecture. For example, information exchange in traditional computer networks relies on the Open System Interconnection (OSI) model. The exchange of information among the OSI computing systems is separated into seven abstraction layers: application, transport, network, MAC, data link, and physical. An underlying communication routing protocols manage each layer. Thus, internetworking management is complex because each router device is responsible for routing, controlling, forwarding, and filtering packets (Sarhan, Jemmali & Ben Hmida, 2021). Furthermore, IP addresses and domain name systems (DNS) are not decentralized. Thus, it is a single point of failure [44]. Such a complicated, insecure traditional model needs to be secure and simplified. Several technologies have been proposed to simplify such a complex paradigm (Jemmali & Ben Hmida, 2021; Sawalmeh & Othman, 2018) for instance, Delay-tolerant Networking (DTN), and Software-Defined Networking (SDN).

The idea of fixing the Internet by dealing with the broken design and architecture of the current internetworking and building a new network from scratch has launched several funded projects, as cited in (Lan et al., 2022). The projects are as follows: the Future Internet Design (FIND), the Global Environment for Networking Innovations (GENI), the future Internet research and experimentation (FIRE), AKARI of Japan, Named Data Networking (NDN), 4WARD, MobilityFirst, ChoiceNet, FIRST, NEBULA, and the Service-Customized Networking (SCN) research projects (Lan et al., 2022; Lemin, 2013; Zhang, 2010; Raychaudhuri, Nagaraja & Venkataramani, 2012; Harai, 2009; Brunner, 2010; Wolf, 2014; Jinho, Bongtae & Kyungpyo, 2014; Anderson, 2014; Liu, 2014; Greenberg, 2005). Consequently, future network architecture should contain several core characteristics, including openness, reliability, robustness, controllability, scalability, adaptability, high performance, availability, security, credibility, manageability, highly cost-effective, and ubiquitous services (Lan et al., 2022).

Because of the emerging technologies and the broad technological and research advancements in computer networks and communications, network security vulnerability, risks and threats are gradually expanding. Consequently, the rising number of cyber security attacks, including ransomware, denial-of-service, password, and phishing attacks, has led to massive data breaches and losses in several reputable financial and industrial businesses, including government and military networks. This advancement makes people distrust enterprises, which leads firms to

mistrust traditional tools and safeguards (Xue, Tang & Fang, 2022; Fedele & Roner, 2022; Kärkkäinen, 2015).

Military networks use the public network as the primary means of communication. Thus, it is targetable for several threats, including vulnerabilities and cybersecurity attacks. Developing a military-based Network-enabled capability in a reasonable time is unrealistic due to the complexity of global internet governance. For example, in 2019, the US government banned Huawei—a major telecom giant company, to prevent China from having superior control over cyberspace governance (Kärkkäinen, 2015; Tang, 2020). Hence, there is a need for a partial resolution like designing secure network architectures that can provide a timely solution in response to urgent protection needs in such a critical armed force environment. This network should provide multilevel security, privacy protection, and delay-tolerant networking (Kärkkäinen, 2015).

This paper aims to propose a two-routers network-based cyber security architecture that offers private and secure multilevel data sharing. Hence, we develop a number of algorithms to achieve the goal of this paper. The proposed algorithms can be applied to enhance the monitoring system developed by (Melhim et al., 2020; Melhim et al., 2019). On the other hand, the algorithms developed by (Jemmali et al., 2019; Alharbi & Jemmali, 2020; Jemmali, 2021; Jemmali et al., 2020) can be utilized to be extended by the proposed problem. Our solution suggests enhancing the current IP network architecture by providing multilevel data security and privacy protection. However, other issues in the existing IP network architecture are outside the scope of this research. Our approach has the following pros: (i) employs algorithmic techniques for future private networks; (ii) provides support for anonymous communication and secure and anonymous data sharing during a crisis and in various domains like the military, pandemics, journalism, and news coverages; (iii) presents several approximate algorithms for an NP-hard problem and uses it for secure data dissemination; (iv) uses known and unknown algorithmic techniques such as randomization method, iterative approach and probabilistic method; (v) presents good optimal time for the problem as it shown in the result section.

To be specific, assume a journalist wants to report private information about a violation anonymously during *a military disaster*, natural disaster, health pandemic, earthquake, flood, etc. Furthermore, suppose such confidential information demands to be communicated anonymously and promptly. In that case, there will be a need for a novel architecture that minimizes the risk of such highly confidential information breaches. Our scheme includes the following drawbacks. (1) The proposed problem is difficult; hence solving it via n-hops might be complex and requires advanced algorithmic techniques of big O complexities. (2) There is a need to use a lower bound in a branch-and-bound algorithm to develop an exact solution for the problem. The following section discusses the related work. Next, we describe the problem definition. Following, we show the architecture and design of the proposed approach. After that, we introduce the proposed algorithms, report the results, and discuss the performance measurement. Finally, we summarize the paper and discuss future work.

Literature Review

An Overview of Current and Future Network-Based Technologies Challenges

An old or traditional computer network is a hardware-based or physical network that employs protocols based on the TCP/IP suite and requires several network devices, such as switches and routers, for growth. This interconnected system, the "Internet," has expanded worldwide since its

establishment. However, its complex nature has made it undesirable due to several challenges like flexibility, security, connectivity, complexity, and bandwidth. On the other hand, computer networks nowadays pay significant attention because of the wide adoption of new features and technologies like automaticity, AI, cloud computing, machine learning, SDN, and IoT.

SDN has been considered by many as one of the possible future network paradigms due to its benefits in strengthening network architecture, reducing operational costs, and supporting the addition of new applications and functions. SDN is a software-based architecture that simplifies and improves network control by isolating the control from the forwarding plane, thus making it practical to add new network functions or protocols. However, SDN possesses security concerns and other issues (Benzekki, El Fergougui & Elbelrhiti Elalaoui, 2016; Shin et al., 2016; Duan, Yan, and Vasilakos, 2012; Lan et al., 2022). Therefore, SDN is used by (Shin et al., 2016) to enhance network security and information security processes. Since SDN is considered the foundational building block of Intent-Based Networking (IBN), it is being functioned to address SDN's shortfall. For example, IBN proposed to deal with system requirements without going into detail. In IBN, the system behaviors are chosen by rules which are considered a kind of policy. The current focus on IBN is still inside academia. However, there is an expectation for future adoption of IBN by leading cloud vendors due to advancements in AI, specifically in natural processing language (NLP)(Rafiq, Afaq & Song, 2020; Zeydan & Turk, 2020).

The fifth-generation technology (5G) wireless network aims to address 4G challenges such as; data rate, spectral and energy efficiency, capacity, and Quality of Service (Gupta & Jha, 2015). However, 5G has issues like authentication and data security (Sivasubramanian, Shastry & Hong, 2022).

Cloud computing is a collection of shared resources that includes computer networks, storage, services, and servers. The three standard cloud computing service paradigms are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which can be managed and hosted through an independent third-party provider and accessed through the Internet. Cloud networking is concerned with methods to access cloud applications. It can be accessed and operated through personal and BYOD devices like desktop computers and other "BYOD" interfaces or personal devices that can access the Internet, like laptops, smartphones, and personal computers (Hong et al., 2019). Besides maintenance and cost saving, efficiency, and workload flexibility, the cloud enables organizations from various domains to share and exchange data for performing analysis and extracting patterns that can find solutions for multiple problems (Sarhan & Carr, 2017). Accessing cloud computing can be through one or more efficient deployment models: private, public, hybrid, or multi-cloud. Cloud technology has many challenges and drawbacks presented as follows: (i) Centralization (external third party manages data computation and storage); (ii) High Latency; (iii) Interoperability; (v) Data security, privacy, and management. Unlike the hybrid cloud, which relies on multiple deployment modes, the multi-cloud technology model utilizes various cloud services simultaneously from multiple cloud service providers. It addresses challenges presented in other cloud models (Hong et al., 2019).

The age of the Internet of Things (IoT) has made a massive number of devices connect to the cloud bringing several issues related to cloud centralization. Edge computing can overcome problems related to the centralization nature of the cloud, such as network bandwidth and bandwidth cost, latency, IoT battery life constraints, and privacy because the data processing and computation happen at the network's edge (Shi et al., 2016). However, the drawback of Edge Computing is the security (Jiang et al., 2015; Hossain, Fotouhi & Hasan, 2015; Yang et al., 2017). Cloud

Repatriation is a new concept proposed to overcome security issues in the cloud. Compared to edge computing, cloud repatriation eliminates issues possessed by the public cloud, like operation cost, performance, control, and security (Shin et al., 2016; Hintemann, 2020). However, Cloud Repatriation is still under consideration.

Network Security Challenges

The current network security challenges have resulted from the poor, insecure traditional complex architecture of the Internet. As a result, several approaches have been presented to provide architectures for such issues. For instance, Casado et al. published a scheme for protecting network architecture. The so-called "SANE" scheme provides strict security policy control for private networks. It prevents illegal interaction and requires the source and destination to be declared (Casado et al., 2006).

XIA aims to provide a single network infrastructure that controls the network and removes communication obstacles between the end users and the network infrastructure. It uses an application program interface (API) for port-to-port communication. The security mechanism in XIA, the so-called "intrinsic security mechanism," is implemented through a unified network infrastructure in which each user has security identification applied to credit management. Furthermore, the security control in XIA increases from single packet forwarding to interoperation among the network components (Berman et al., 2014).

NEBULA aims to provide built-in security and adaptable central network architecture that uses cloud computing data centers for storing and computing data. As a result, it can solve cloud computing's emerging security threats (Liu et al., 2014). FIRE aims to provide network architecture and protocols for future intelligent Internet that address security, complexity, scalability, and mobility issues. Its interconnected smart networks should support intelligent transportation, medical, and social life (Gavras et al., 2007). MobilityFirst focus on providing mobile services architecture to design future Internet based on mobile devices. Its main intention is to address security, privacy, availability, manageability, and tolerance (Naylor et al., 2014).

Packets Security and Privacy Challenges

Alzahrani et al. (Alzahrani & Chaudhry, 2022) proposed an SDN securing source routing forwarding scheme that provides packet protection by using a cryptographic authenticator to authorize SDN switches and impose a selected routing path. Their approach uses identity-based encryption (IBE), considers single and multipath transmissions, and allows the receiver to authenticate the envisioned path of the forwarded packets. The drawback of their scheme is the security-performance overhead.

Zeng et al. (Zeng, Zhang & Xia, 2022) proposed a blockchain-based SDN network architecture for the security of routing among numerous hosts. However, their scheme relies on the reputation concept for routing reliability which cannot be absolute. Legner et al. (Legner et al., 2020) proposed EPIC protocols to secure the interdomain paths at the Internet inter-autonomous communication system levels. They used symmetric key encryption for packet authentication between the sender and receiver at the network layers. Finally, Singh et al. (Singh et al., 2021) proposed a secure scheme that controls the traffic flow by integrating blockchain with switches. Their solution uses deep learning and a zero-knowledge proof technique to verify the registered switches in the network.

Multilevel Data Sharing Approaches

Zaghloul et al. suggested a cloud-secure and efficient multilevel data outsourcing solution. The

scheme partitions the outsourced data into different parts to share it according to (i) the user's authorized privileges and (ii) the level of confidentiality of the outsourced data (Zaghloul, Zhou & Ren, 2020).

Sarhan et al. proposed a novel multilevel data-outsourcing approach to protect outsourced data in the cloud. The scheme uses Secure Multi-Party Computation, ciphertext policy attribute-based encryption (CP-ABE), and active bundles to encapsulate the data with its access policy within a virtual machine. Besides using CP-ABE that permits multilevel data access, the schemes encapsulate two attributes: location and time to strengthen the protective layer for the outsourced data in the cloud (Sarhan & Lilien, 2014; Sarhan & Carr, 2017; Sarhan, Jemmali & Ben Hmida, 2021; Sarhan, 2017).

Our Approach Versus the Other Two Routers' Approaches

Alquhayz et al. approach uses a scheduler for packet prioritizing based on data multilevel security constraints. They proposed Several heuristics and performed simulation experimentation using a static window pass based on a single router (Jemmali & Alquhayz, 2020; Alquhayz & Jemmali, 2021). In other work (Jemmali & Alquhayz, 2020), they used identical routers for scheduling problems.

Sarhan et al. packet multilevel security scheme uses a constraint-based packet categorization and dissemination and two routers. In addition, the authors proposed several scheduling algorithms to minimize the transmission time (Sarhan, Jemmali & Ben Hmida, 2021; Sarhan & Jemmal, 2022). This research uses different heuristics to deal with the proposed problem.

Problem Formulation

We target the problem of protecting multilevel packets by controlling the packets' path and transmission time, which is essential in a private network. We assume that the network packets are classified into several classification levels so that packets belonging to the identical classification level are prohibited from being transmitted at the same time over the two routers. This problem is a difficult problem that we handle using approximate solutions. Furthermore, we impose a security constraint that prevents two packets from the same confidential level from transiting simultaneously to maximize the level of outsourced data protection and minimize the chances of data leaks.

The objective of this paper is to create numerous near-optimal solutions for the studied problem. We refer to Pt as a group of packets and mark n as their number. We denote $R1$ for router1 and denote $R2$ for router 2. When packet Pt_j is sent to router $R1$, the cumulative transmission time is denoted as Ct_j^1 and when packet Pt_j is assigned to the router $R2$, the cumulative transmission time is denoted as Ct_j^2 . We denote t_j for packet Pt_j estimated transmission time. See Table 1 for more details. We denote T_1 and T_2 for the total time of transmission on $R1$ and $R2$, and T_m for the routers' maximum time, so $T_m = \max(T_1, T_2)$. Cg_i denotes the categories such that $i = \{1, \dots,$

251 n_{cg} and n_{cg} is the number of categories fixed by the administrator. The objective is to minimize
 252 T_m .

253 **Table 1:**
 254 **System Notation Summary**

255 **Proposition**

256 Two routers scheduling problem based on multilevel security is a difficult problem because the
 257 minimization of the total time of transmission using the 2-routers problem is the reduction 2-
 258 parallel machines NP-Hard problem (Sarhan, Jemmali & Ben Hmida, 2021; Garey & Johnson,
 259 1979). This reduction is because the two routers correspond to the two machines, and the
 260 scheduling of packets corresponds to the scheduling of jobs.

261 **Architecture and Design**

262 This section provides the proposed solution architecture details and its objective design.

263 **System Model**

264 This sub-section discusses the components of the proposed two-routers network-based cyber
 265 security architecture. In figure 1, the constructed architecture assumes the transmissions of packets
 266 using two routers. The processes are as follows: first, the data owner and decision maker (e.g.,
 267 machine learning engine or agent) categorize the data into several classified levels. Next, the
 268 categorized data will be waited in a buffer and processed by a scheduler via a selected algorithm
 269 from a pool, which intelligently controls the packet transmitted to the two routers. The scheme is
 270 composed of several components described as follows:

- 271 1) Data Owner: This component manages the transmitted data's classified level, specifies the files
 272 to be sent to the key decision maker, and fixes the data level categories.
- 273 2) Decision Maker: This component represents a key decision maker, or security policy maker,
 274 who categorizes the transmitted data and their level of importance.
- 275 3) Smart Engine: This component represents a software agent that manages data transmission to
 276 the data buffer. It controls this component, administers the data and its transmission, and links the
 277 sent files with their categories after being classified.
- 278 4) Data Collection engine: This component groups all files for the transmitted data.
- 279 5) Data Buffer engine: This component collects, verifies, and links the sent files within a
 280 category.
- 281 6) Scheduler: This component is essential for solving a scheduling problem related to data
 282 disclosure through two routers. The scheduler provides several algorithms and selects the best one
 283 to solve a particular scheduling problem. It receives the files sent from the Data buffer engine.
- 284 7) Receiving buffer: This component stores or groups the transmitted files in the 'Receiver buffer.'

8) Routers: This component represents the two routers.

9) Receiver: This component represents a user expecting to receive confidential information.

Design Objective

To provide a secure future network architecture that offers multilevel data sharing for future deployment of private networks in a critical environment. Our design objectives are as follows:

(i) Multilevel data access policy: Designing a multilevel security policy for data classification and transmission. Note that a constraint governs the security policy and the transmitted packets.

(ii) Scheduler: Designing a scheduler capable of selecting the best packet scheduling algorithm from a pool. The scheduler is assumed to perform its calculations autonomously.

(iii) Two routers: Designing a network paradigm such that the classified packets do not significantly impact the transmission time.

Figure 1: Two routers architecture for secure packet dissemination

Proposed Algorithms

This section presents five newly designed algorithms that solve the studied problem (Sarhan, Jemmali & Ben Hmida, 2021; Sarhan & Jemmal, 2022) in a remarkable time. The proposed algorithms use different techniques to enhance the transmitted time and reduce the algorithmic complexity. The first discussed algorithm is the "longest transmission time with excluding the first and last packet" (LTFL). In LTFL, packets are arranged in descending sequence to exclude the longest and shortest packets with estimated transmission time and then to schedule all remaining packets. Next, we describe "the shortest transmission time with excluding the first and the last packet" (STFL) algorithm. In STFL, we arrange packets in ascending sequence to exclude the longest and shortest packets with estimated transmission time, so the obtained schedule will be used to calculate the result. Third, we discuss the "Shortest-Grouped classification" (SG) algorithm. In SG, we arrange packets in ascending sequence based on their estimated transmission time, and then we divide them into groups to schedule them through several variants to find a better solution than others. After that, we talk about the "Random-Grouped classification with longest scheduling" (RGL) algorithm, and finally, we present the "Random-Grouped classification with shortest scheduling" (RGS) algorithm. Unlike SG, In RGL and RGS sorting, the packets are delayed until the end to pick the best solution.

Longest Transmission Time with Excluding the First and the Last Packet (LTFL)

In LTFL, the processes are as follows: First, we store packets in decreasing order based on their approximate transmission time descending sequence. Next, we exclude the longest and the shortest packets. Third, we schedule the $n-2$ remaining packets on the faster or lowest completed-time router, and finally, we schedule the two retained packets. Note that $Dsc()$ denote the function that sorts all packets according to their estimated transmission time descending sequence, and $Schd(L)$ denotes the function that schedules a list L on the two routers.

Algorithm 1:

Algorithm LTFL

Shortest Transmission Time with Excluding the First and the Last Packet (STFL)

In STFL, the processes are as follows: First, we sort the packets according to the increasing order

of their estimated transmission time. Second, we exclude the longest and the shortest packets. Next, we schedule the $n-2$ remaining packets on the router with the minimum completion time, and finally, we schedule the two retained packets. Note that $Isc()$ denote the function that sorts all packets according to the increasing order of their estimated transmission time.

Algorithm 2:

Algorithm STFL

Shortest-Grouped classification algorithms (SG)

In SG, the processes are as follows: First, we sort the packets corresponding to the estimated transmission time ascending sequence. Next, we divide the sorted packets into three groups such that each group is composed of $\frac{n}{3}$ packets. The first group $G1$ contains the first $\frac{n}{3}$ packets, the second group $G2$ contains the second $\frac{n}{3}$ packets, and the last group, $G3$ contains the remaining packets. Third, we adopt four variants to schedule the packets in these groups. We denote SG_1 for the first variant. The schedule of SG_1 packets are applied as follows: we schedule packets of $G2$, next packets of $G1$, and finally packets of $G3$. This variant is denoted by SG_1 . We denote SG_2 for the second variant. The schedule of SG_2 packets are applied as follows: we schedule packets of $G2$, next packets of $G3$, and finally packets of $G1$. We denote SG_3 for the third variant. The schedule of SG_3 packets are applied as follows: we schedule packets of $G3$, next packets of $G1$, and finally packets of $G2$. We denote SG_4 for the fourth variant. The schedule of SG_4 packets are applied as follows: we schedule packets of $G1$, next packets of $G3$, and finally packets of $G2$.

Hereafter, we denote $Gprd()$ for the function that returned the three lists related to $G1$, $G2$, and $G3$. These lists will be denoted respectively by $SG1$, $SG2$, and $SG3$.

Algorithm 3:

Algorithm SG_1

Algorithm 4:

Algorithm SG_2

Algorithm 5:

Algorithm SG_3

Algorithm 6:

Algorithm SG_4

Random-Grouped Classification with Longest Scheduling Algorithms (RGL)

As detailed in the above subsection, we first divide the packets (without any sorting) into three groups. Then, we apply the same four variants described above to schedule the packets in these

groups. Finally, packets are sorted in each group according to their estimated transmission time decreasing order. Note that the first, second, third, and fourth variants are denoted by RGL_1 , RGL_2 , RGL_3 , and RGL_4 , respectively.

Algorithm 7:

Algorithm RGL_1

Random-Grouped Classification with Shortest Scheduling Algorithms (RGS)

As detailed in the above subsection, we divide the packets (without any sorting) into three groups. Then, we apply the same four variants described above to schedule the packets in these groups. Finally, packets are sorted in each group according to their estimated transmission time increasing order. Note that the first, second, third, and fourth variants are denoted by RGS_1 , RGS_2 , RGS_3 , and RGS_4 , respectively.

Algorithm 8:

Algorithm RGS_1

Experimental Setup

The section describes the proposed algorithms' experimental results, the variables used, and the Simulation environment to measure the performance.

We used C++ to prototype the proposed algorithms. The computing environment included one gigahertz on an Intel CPU and eight gigabytes of RAM. We produced 300 instances defined as follows: $n = \{15, 25, 35, 45, 55\}$ and $n_{cg} = \{2, 3, 5\}$ to measure the created algorithms' performance measurements. We used a random function called a uniform distribution to generate the estimated transmission time. We denote $U[.]$ for the uniform distribution function.

In this paper, we adopt two classes. Class 1 corresponds to the estimated transmission time generated as $U[1 - 50]$. Class 2 corresponds to the estimated transmission time generated as $U[1 - 100]$. For each pair (n, n_{cg}) and for each class, we produce ten instances; thus, we calculate the total number of instances as follows: $5 \times 3 \times 2 \times 10 = 300$ instances. Furthermore, we used three variables to evaluate the created algorithms' performance time. The descriptions of the variables are as follows; (i) variable Prc indicates the total instances percentage in case a given algorithm is the same as the best; (ii) variable Dv indicates the gap between a candidate algorithm value, say " x " and the best-obtained one value say " y ". Indeed, $Dv = \frac{x-y}{y}$. (iii) variable Tm represents the algorithm's average time in seconds. Note that the mathematical symbol "-" indicates that the time is lower than 0.001 s.

Results & Discussion

This section describes the experimental findings of the created algorithms. Then, compare the results with those presented in (Sarhan, Jemmali & Ben Hmida, 2021; Sarhan and Jemmal, 2022) to find the best algorithm. A summary of the core experimental variables and performance results is in Table 2, Table 3, Table 4, Table 5, and Table 6. Table 2 presents an overview of the performance of the proposed algorithms in this paper. Our observation is that the best algorithm

is the Random-Grouped Classification with Shortest Scheduling Algorithms (*RGS*) since its first and fourth variants (RGS_1 and RGS_4) achieved the best results recording 37.7%, an average gap of 0.03, and an estimated transmission time of 0.001 s. We also notice that the worst algorithm is *STFL*, rating 18.3 %, a gap of 0.04, and an estimated transmission time of 0.001, and the lowest average gap algorithm is SG_2 . *Table 3* compares the variations of the average gap of all proposed algorithms when n changes. We observe that both algorithms' *STFL*, and SG_1 average gap variations are alike regardless of the number of packets n . Moreover, algorithm SG_2 has the lowest average gap variation of 0.01 in two scenarios when $n=45$ and $n=55$. On the other hand, the average gap variation for algorithm *LTFL* increases when n is low. For example, the highest average gap of 0.07 appears with algorithm *LTFL* when $n=15$. *Table 4* shows that all algorithms have the same average gap variation of 0.01 when $n_{cg}=2$ except algorithm SGL_2 which is equal to 0.02. Furthermore, algorithms SGL_3 and SGL_4 have the same average gap variation regardless of the changes in the number of categories n_{cg} . *Table 5* presents the time variation for all proposed algorithms when n changes. We observe that the time variation for the algorithm SGL_2 do not get impacted by the changes in the number of packets n since it equals 0.001. One should also observe that the time variation for algorithm *LTFL* gradually decreases when the number of packets n increases, and the time variation for both algorithms SGL_2 and SG_2 are alike or do not change when the number of packets n changes. *Table 6* displays the proposed algorithms' variation of time when n_{cg} changes. It is observable that both algorithms SGS_2 and SG_4 time variation does not get impacted by the changes in the number of categories n_{cg} variation since $SGS_2=0.001$ and $SG_4=0.002$ regardless of the value of n_{cg} . One should also observe that the time variation for algorithm *LTFL* gradually increases when the value of n_{cg} increases. Furthermore, the time variation for algorithms SG_2 , SG_3 , RGS_1 and RGS_2 are alike regardless of the changes in the number of categories n_{cg} . Finally, the time variation for algorithms SG_1 , SGL_1 are alike regardless of the changes in n_{cg} .

In this paper, we proposed a group of algorithms that give remarkable results. We compare the results with those (Sarhan, Jemmali & Ben Hmida, 2021; Sarhan and Jemmal, 2022). We denote B_{new} for the algorithm that returns the best value of all proposed algorithms—running the best algorithm MDETA developed in (Sarhan, Jemmali & Ben Hmida, 2021) on the 300 used instances. The experimental results show that for 61 instances, $B_{new} < MDETA$. This result means that B_{new} participates in giving a better solution with MDETA. Furthermore, for 134 instances, we have $B_{new} = MDETA$. On the other hand, comparing the results given by the proposed algorithms with the best algorithm \overline{RLT} developed in (Sarhan and Jemmal, 2022), the results show that for 13 instances, we have $B_{new} < \overline{RLT}$. This result means that B_{new} participates in giving a better solution with \overline{RLT} . Besides that, for 116 instances, we have $B_{new} = \overline{RLT}$. Note that the proposed scheme packets protection mechanism is achieved through imposing a constraint or restrictions for the transmission of packets using a smart security policy. The *multilevel* security policy assigns security levels called categorizations to packets and uses a scheduler to control their dissemination route and dissemination time via the two routers to minimize the chances of breaches. Packets

belong to the same classification level are forbidden from being transmitted at the same time over the two routers.

Table 2:

Overview of the performance of the proposed algorithms

Table 3:

The proposed algorithms gap variation related to the number of packets

Table 4:

The proposed algorithms gap variation related to the number of categories

Table 5:

The proposed algorithms time variation in seconds related to the number of packets

Table 6:

The proposed algorithms time variation in seconds related to the number of categories

Conclusions

Multilevel security is one of the essential features required in future and special-purpose networks. In this research, we propose a multilevel secure network model using two machines that can transmit confidential data in a private environment or in particular circumstances like a crisis based on a security policy. The scheme uses a scheduler to securely minimize the transmitted time when disseminating the multilevel secure packets. We proposed several heuristics for this NP-Hard problem. Our experimental results show promising results for the future development of our paradigm. Both RGS_1 and RGS_4 showed promising results. We plan for future work to increase the number of routing machines to n machines and modify our paradigm as network as a service (NaaS). We also plan for future work to demonstrate our approach in the application layer using a private set intersection and agent-based solutions to provide an anonymous interaction during crisis management.

References

- Benzekki K, El Fergougui A, and Elbelrhiti Elalaoui A. 2016. Software-defined networking (SDN): A survey. *Security and Communication Networks*, vol. 9, no.18, pp. 5803–5833. DOI. <http://dx.doi.org/10.1002/sec.1737>
- Shin S, Xu L, Hong S, and Gu G. 2016. Enhancing network security through software defined networking. (SDN). In: Proceedings of the 25th International Conference on Computer Communications and Networks (ICCCN), pp. 1-9.
- Duan Q, Yan Y, Vasilakos A V. 2012. A survey on service-oriented network virtualization toward convergence of networking and cloud computing. *IEEE Transactions on Network and Service Management*. vol. 9, no. 4, pp. 373-392.
- Lan J L, Hu Y, Zhang Z, Jiang Y, Wang P et al. 2022. Future Network Architectures and Core Technologies. Singapore, Singapore: World Scientific. Available at <https://www.worldscientific.com/worldscibooks/10.1142/12297>.
- Shi W, Cao J, Zhang Q, Li Y, and Xu L. 2016. Edge computing: Vision and challenges. *IEEE internet of things journal*, vol. 3, no. 5, pp. 637-646.
- Jiang H, Shen F, Chen S, Li K-C, and Jeong Y.-S. 2015. A secure and scalable storage system for aggregate data in IoT. *Future Generation Computer Systems*. vol. 49, pp. 133-141.
- Hossain M M , Fotouhi M, and Hasan R. 2015. Towards an analysis of security issues, challenges, and open problems

- 475 in the Internet of Things. In: Proceedings of IEEE World Congress on Services. (SERVICES). pp. 21_28.
- 476 Yang X, Wang T, Ren X, and Yu W. 2017. Survey on improving data utility in differentially private sequential data
477 publishing. *IEEE Transactions on Big Data*. vol. 7. no. 4. pp. 729-749.
- 478 Sarhan A Y , and Carr S. 2017. A highly-secure self-protection data scheme in clouds using active data bundles and
479 agent-based secure multi-party computation. In: Proceedings of the 4th International Conference on Cyber Security
480 and Cloud Computing (CSCloud). pp. 228-236.
- 481 Lemin Li. 2013. Future Network Architectures. *ZTE Technology Journal*. vol. 19, no. 6, pp. 39–42.
- 482 Hintemann R. 2020. *Efficiency Gains are Not Enough: Data Center Energy Consumption Continues to Rise*
483 *Significantly*. Berlin, Germany: Borderstep Inst. for Innovation and Sustainability. Available at
484 https://www.borderstep.de/wp-content/uploads/2020/04/Borderstep-Datacenter-2018_en.pdf
- 485 Mitra A, and Chaurasia R. 2022. *Emerging Technologies and Global Pandemic*. In: *Global Pandemic and Human*
486 *Security: Technology and Development Perspective* 1st ed., Singapore: Springer. pp. 367-391.
- 487 Hong J, Dreibholz T, Schenkel J A, and Hu J A. 2019. An overview of multi-cloud computing. In: Proceedings of the
488 international conference on advanced information networking and applications (AINA). Matsue, Japan, pp. 1055–
489 1068.
- 490 Rafiq A, Afaq A and Song W C. 2020. Intent-based networking with proactive load distribution in data center using
491 IBN manager and Smart Path manager. *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11,
492 pp. 4855-4872.
- 493 Zeydan E, and Turk Y. 2020. Recent advances in intent-based networking: A survey. In: Proceedings of IEEE 91st
494 Vehicular Technology Conference (VTC2020-Spring). Antwerp, Belgium, pp. 1-5.
- 495 Gupta A, and Jha R K. 2015. A survey of 5G network: Architecture and emerging technologies. *IEEE access*, vol. 3,
496 pp. 1206-1232.
- 497 Sivasubramanian A, Shastry P N, and Hong P C. 2022. Futuristic Communication and Network Technologies.
498 *Springer Nature*.
- 499 Sarhan A Y and Lilien L T. 2014. An Approach to Identity Management in Clouds without TrustedThird Parties.
500 *Transaction of the 11th Western Michigan IT Forum*. vol. 1. no. 1, pp. 18-27.
- 501 Sarhan A, Jemmali M, and Ben Hmida A. 2021. Two routers network architecture and scheduling algorithms under
502 packet category classification constraint. In: Proceedings of the 5th International Conference on Future Networks &
503 Distributed Systems (ICFNDS-'21). Dubai, UAE, pp. 119-127.
- 504 Sarhan AY. 2017. "Protecting Sensitive Data in Clouds Using Active Data Bundles and Agent-Based Secure Multi-
505 Party Computation." Ph.D. dissertation, Western Michigan University.
- 506 Xue R, Tang P, and Fang S. 2022. Prediction of Computer Network Security Situation Based on Association Rules
507 Mining. *Wireless Communications and Mobile Computing*. vol. 2022.
- 508 Luo J. 2022. Data-Driven Innovation: What Is It. *IEEE Transactions on Engineering Management*. to be published.
509 doi: 10.1109/TEM.2022.3145231.
- 510 Fedele A, and Roner C. 2022. Dangerous games: A literature review on cybersecurity investments. *Journal of*
511 *Economic Surveys*. vol. 36. no. 1. pp. 157-187.
- 512 Sawalmeh A H, and Othman N S. 2018. An overview of collision avoidance approaches and network architecture of
513 unmanned aerial vehicles (UAVs). *International Journal of Engineering & Technology*. vol. 7. no. 4.35. pp. 924–
514 934.
- 515 Casado M, Garfinkel T, Akella A, Freedman M J, Boneh D, et al. 2006. SANE: A protection architecture for enterprise
516 networks. In: Proceedings of the USENIX Security Symposium (USENIXSS'06). pp. 137–151.
- 517 Zhang L, Estrin D, Burke J, Jacobson V, Thornton J D et al. 2010. Named data networking (NDN) project. Relatório
518 Técnico NDN, Xerox Palo Alto Res, Center-PARC. vol. 157. pp. 158.
- 519 Raychaudhuri D, Nagaraja K, and Venkataramani A. 2012. Mobilityfirst: a robust and trustworthy mobility-centric

- 520 architecture for the future internet. *ACM SIGMOBILE Mobile Computing and Communications Review*. vol.16. no.3.
521 pp. 2-13.
- 522 Naylor D, Mukerjee M K, Agyapong P, Grandl R, Kang R et al. 2014. XIA: architecting a more trustworthy and
523 evolvable internet. *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3. pp. 50-57.
- 524 Berman M, Chase J S, Landweber L, and Nakao A. 2014. GENI: A federated testbed for innovative network
525 experiments. *Computer Networks*. vol. 61. no. 1. pp.5-23.
- 526 Gavras A, Karila A, Fdida S, and May M. 2007. Future internet research and experimentation: The FIRE Initiative.
527 *ACM SIGCOMM Computer Communication Review*. vol. 37. no. 3. pp. 89-92.
- 528 Harai H. 2009. AKARI architecture design for new generation network. In: Proceedings of 2009 IEEE/LEOS Summer
529 Topical Meeting (LEOSST-09). pp. 155-156.
- 530 Brunner M, Abramowicz H, Niebert N, and Correia L M. 2010. 4WARD: A European perspective towards the future
531 Internet. *IEICE Transactions on Communications*. vol. 93. no. 3. pp. 442-445.
- 532 Wolf T, Griffioen J, Calvert K L, Dutta R, Rouskas G N et al.2014. ChoiceNet: toward an economy plane for the
533 Internet. *ACM SIGCOMM Computer Communication Review*. vol. 44. no. 3. pp. 58-65.
- 534 Jinho H, Bongtae K, and Kyungpyo J.2009. The study of future internet platform in ETRI. *The Magazine of the IEEE*.
535 vol. 36, no. 3, pp. 68-74.
- 536 Anderson T, Birman K, Broberg R, Caesar M, Comer D et al.2014. A brief overview of the NEBULA future Internet
537 architecture. *ACM SIGCOMM Computer Communication Review*. vol. 44. no. 3. pp. 81-86.
- 538 Liu Y J, Huang T, Zhang J, Liu J, Yao H P et al. 2014. Service customized -networking. *Journal on Communications*.
539 vol. 35. no. 12. pp. 1-9.
- 540 Greenberg A, Hjalmtysson G, Maltz D, Myers A, Rexford J et al. 2005. A clean slate 4D approach to network control
541 and management. *ACM SIGCOMM Computer Communication Review*. vol. 35. no. 5. pp. 41-54.
- 542 Ballani H, and Francis P. 2007. CONMan: A step towards network manageability. *ACM SIGCOMM Computer
543 Communication Review*. vol. 37. no. 4. pp. 205-216.
- 544 Alzahrani B and Chaudhry S A. 2022. An Identity-Based Encryption Method for SDN-Enabled Source Routing
545 Systems. *Security and Communication Networks*. vol. 2022. pp. 1-7.
- 546 Zeng Z, Zhang X, and Xia Z. 2022. Intelligent blockchain-based secure routing for multidomain SDN-enabled IoT
547 networks. *Wireless Communications and Mobile Computing*. vol. 2022, pp. 1-10.
- 548 Legner M , Klenze T, Wyss M, Sprenger C, and Perrig A. 2020. EPIC: every packet is checked in the data plane of a
549 path-aware internet. In: Proceedings of the 29th USENIX Security Symposium (USENIX Security 20). pp. 541-558.
- 550 Singh M, Aujla G S, Singh A, Kumar N, and Garg S. 2021. Deep-learning-based blockchain framework for secure
551 software-defined industrial networks. *IEEE Transactions on Industrial Informatics*. vol. 17, no. 1, pp. 606-6161.
- 552 Kärkkäinen A. 2015. Developing cyber security architecture for military networks using cognitive networking. Ph.D.
553 dissertation. Aalto University, Finland.
- 554 Tang M. 2020. Huawei versus the United States? The geopolitics of extraterritorial internet infrastructure. *International
555 journal of communication*. vol. 14, pp. 4556-4577.
- 556 Zaghloul E, Zhou K and Ren J. 2020. P-MOD: Secure Privilege-Based Multilevel Organizational Data-Sharing in
557 Cloud Computing. *IEEE Transactions on Big Data*. vol. 6. no. 4. pp. 804-815.
- 558 Jemmali M and Alquhayz H. 2020. Equity data distribution algorithms on identical routers. In *Proc. ICICC 2019*,
559 Ostrava, Moravian-Silesian Region, Czech Republic, pp. 297-305, 2020.
- 560 M. Jemmali and H. Alquhayz. 2020. Time-slots transmission data algorithms into network. In: Proceedings of the
561 2020 International Conference on Computing and Information Technology (ICCIT-1441). pp. 1-4, 2020.
- 562 Alquhayz H and Jemmali M. 2021. Fixed Urgent Window Pass for a Wireless Network with User Preferences.
563 *Wireless Personal Communications*. vol. 120. no.2. pp. 1565-1591.

- 564 Garey M R and Johnson D S. 1979. *Computers and Intractability: A Guide to the Theory of NP Completeness*. 1st ed.
565 vol. 174. New York, NY, USA: W. H. Freeman & Co.
- 566 Sarhan A. and Jemmali M. 2022. Novel intelligent architecture and approximate solution for future networks, *PLOS*
567 *ONE*, Accepted.
- 568 Melhim L, Jemmali M, AsSadhan B, and Alquhayz H. 2020. Network traffic reduction and representation.
569 *International Journal of Sensor Networks*. Vol. 33, no. 4. pp. 239-249.
- 570 Melhim L, Jemmali M and Alharbi M. 2019. Network Monitoring Enhancement based on Mathematical Modeling.
571 In: Proceedings of the 2nd International Conference on Computer Applications & Information Security (ICCAIS). pp.
572 1-4.
- 573 Jemmali M. 2019. Budgets Balancing Algorithms for the Projects Assignment, *International Journal of Advanced*
574 *Computer Science and Applications*. vol. 10, no. 11.
- 575 Alharbi M and Jemmali M. 2020. Algorithms for Investment Project Distribution on Regions. *Computational*
576 *Intelligence and Neuroscience*. vol. 2020.
- 577 Jemmali M. 2021. An optimal solution for the budgets assignment problem. *RAIR-Operations Research*. Vol. 55.
578 no. 2. pp. 873-897
- 579 Jemmali M, Ootom M, and al Favez F. 2020. Max-Min Probabilistic Algorithms for Parallel Machines. In:
580 Proceedings of the 2020 International Conference on Industrial Engineering and Industrial Management. pp. 19-24.
- 581 Al-Gburi A, Abdullah O, Sarhan A, and Al-Hraishawi H. 2022. Channel Estimation for UAV Communication
582 Systems Using Deep Neural Networks. *Drones* vol. 6. no. 11 pp. 326.
- 583 Ali F, Barukab O, Gadicha AB, Patil S, Alghushairy O, Sarhan A. 2022. DBP-iDWT: Improving DNA-Binding
584 Proteins Prediction Using Multi-Perspective Evolutionary Profile and Discrete Wavelet Transform.
585 *Computational Intelligence and Neuroscience*. vol. 2022.

Box 1(on next page)

Algorithm 1: Algorithm LTFL

1

2

```

1    Call Dsc()
2    L1 = the first packet
3    L2 = the last packet
4    L  = all packets excluding L1 and L2
5    Call Schd(L)
6    L3= = {L1, L2}
7    Call Schd(L3)
8    Calculate  $T_m$ 
9    Return  $T_m$ 

```

3

Box 2(on next page)

Algorithm 2: Algorithm STFL

```

1
2
    1    Call Isc()
    2    L1 = the first packet
    3    L2 = the last packet
    4    L  = all packets excluding L1 and L2
    5    Call Schd(L)
    6    L3= = {L1, L2}
    7    Call Schd(L3)
    8    Calculate  $T_m$ 
    9    Return  $T_m$ 
3
4
5

```

Box 3(on next page)

Algorithm 3: Algorithm S_{G_1}

```

1
2
  1  Call Isc()
  2  Call Gprd()
  3  Call Schd (SG2)
  4  Call Schd (SG1)
  5  Call Schd (SG3)
  6  Calculate  $T_m$ 
  7  Return  $T_m$ 
3

```

Box 4(on next page)

Algorithm 4: Algorithm S_{G_2}

1

2

1 Call Isc()

2 Call Gprd()

3 Call Schd (SG2)

4 Call Schd (SG3)

5 Call Schd (SG1)

6 Calculate T_m

7 Return T_m

3

4

Box 5(on next page)

Algorithm 5: Algorithm S_{G_3}

```

1
2
    1  Call Isc()
    2  Call Gprd()
    3  Call Schd (SG3)
    4  Call Schd (SG1)
    5  Call Schd (SG2)
    6  Calculate  $T_m$ 
    7  Return  $T_m$ 
3
4

```

Box 6(on next page)

Algorithm 6: Algorithm S_{G_4}

```

1
2
    1  Call Isc()
    2  Call Gprd()
    3  Call Schd (SG1)
    4  Call Schd (SG3)
    5  Call Schd (SG2)
    6  Calculate  $T_m$ 
    7  Return  $T_m$ 
3
4

```

Box 7 (on next page)

Algorithm 7: Algorithm RGL_1

```

1
2
    1  Call Gprd()
    2  Call Dsc(GL2)
    3  Call Schd (GL2)
    4  Call Dsc(GL3)
    5  Call Schd (GL3)
    6  Call Dsc(GL1)
    7  Call Schd (GL1)
    8  Calculate  $T_m$ 
    9  Return  $T_m$ 
3

```

Box 8(on next page)

Algorithm 8: Algorithm RGS_1

```

1
2
    1  Call Gprd()
    2  Call Isc (GL2)
    3  Call Schd (GL2)
    4  Call Isc (GL3)
    5  Call Schd (GL3)
    6  Call Isc (GL1)
    7  Call Schd (GL1)
    8  Calculate  $T_m$ 
    9  Return  $T_m$ 
3
4
5

```


Table 1 (on next page)

System Notation Summary

Symbol	Description
$R1$	Router 1
$R2$	Router 2
Ct_j^1	the cumulative transmission time when the packet Pt_j is assigned to the router $R1$
Ct_j^2	the cumulative transmission time when the packet j is assigned to the router $R2$
Pt_j	set of packets
n	Number of packets
T_m	maximum completion time on routers
Cg_i	categories with i
n_{cg}	Fixed number of categories

Table 2 (on next page)

Overview of the performance of the proposed algorithms

1

	LTFL	STFL	SG_1	SG_2	SG_3	SG_4	SGL_1	SGL_2	SGL_3	SGL_4	RGS_1	RGS_2	RGS_3	RGS_4
Prc	30.3%	18.3%	24.0%	33.0%	35.0%	23.7%	20.0%	22.7%	23.3%	22.0%	37.7%	37.0%	34.3%	37.7%
dv	0.05	0.04	0.04	0.02	0.03	0.04	0.05	0.04	0.04	0.04	0.03	0.03	0.04	0.03
Tm	0.002	0.001	0.002	0.001	0.001	0.002	0.002	0.001	0.001	0.002	0.001	0.001	0.001	0.001

2

3

4

Table 3(on next page)

The average gap variation for all proposed algorithms when n changes

1

<i>n</i>	LTFL	STFL	<i>SG</i> ₁	<i>SG</i> ₂	<i>SG</i> ₃	<i>SG</i> ₄	<i>SGL</i> ₁	<i>SGL</i> ₂	<i>SGL</i> ₃	<i>SGL</i> ₄	<i>RGS</i> ₁	<i>RGS</i> ₂	<i>RGS</i> ₃	<i>RGS</i> ₄
15	0.07	0.05	0.05	0.04	0.04	0.06	0.05	0.06	0.05	0.06	0.03	0.03	0.03	0.03
25	0.05	0.05	0.05	0.03	0.03	0.04	0.06	0.05	0.04	0.05	0.04	0.04	0.05	0.04
35	0.05	0.04	0.04	0.02	0.03	0.03	0.04	0.04	0.04	0.03	0.03	0.04	0.03	0.03
45	0.04	0.03	0.03	0.01	0.02	0.03	0.03	0.04	0.03	0.03	0.03	0.03	0.03	0.02
55	0.04	0.03	0.03	0.01	0.02	0.02	0.04	0.04	0.04	0.03	0.03	0.03	0.04	0.03

2

Table 4(on next page)

The average gap variation for all proposed algorithms when n_{cg} changes

1

n_{cg}	LTFL	STFL	SG_1	SG_2	SG_3	SG_4	SGL_1	SGL_2	SGL_3	SGL_4	RGS_1	RGS_2	RGS_3	RGS_4
2	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.02	0.01	0.01	0.01	0.01	0.01	0.01
3	0.07	0.06	0.05	0.04	0.05	0.06	0.07	0.06	0.06	0.06	0.05	0.05	0.06	0.05
5	0.07	0.05	0.06	0.02	0.03	0.04	0.06	0.06	0.05	0.05	0.04	0.04	0.03	0.03

2

Table 5(on next page)

The Time variation for all proposed algorithms when n changes

1

<i>n</i>	LTFL	STFL	<i>SG</i> ₁	<i>SG</i> ₂	<i>SG</i> ₃	<i>SG</i> ₄	<i>SGL</i> ₁	<i>SGL</i> ₂	<i>SGL</i> ₃	<i>SGL</i> ₄	<i>RGS</i> ₁	<i>RGS</i> ₂	<i>RGS</i> ₃	<i>RGS</i> ₄
15	0.003	0.001	0.001	0.001	0.001	0.001	0.002	0.001	0.001	0.002	0.001	0.001	0.001	0.001
25	0.002	0.002	0.001	0.001	0.002	0.002	0.001	0.001	0.001	0.002	0.002	0.003	0.001	0.001
35	0.002	0.001	0.002	0.001	0.002	0.002	0.002	0.001	0.002	0.002	0.001	0.000	0.002	0.001
45	0.002	0.002	0.002	0.001	0.001	0.002	0.001	0.001	0.002	0.002	0.001	0.001	0.002	0.002
55	0.001	0.001	0.003	0.001	0.001	0.002	0.002	0.001	0.002	0.002	0.002	0.001	0.001	0.001

2
3

Table 6(on next page)

The Time variation for all proposed algorithms when ncg changes

1

n_{cg}	LTFL	STFL	SG_1	SG_2	SG_3	SG_4	SGL_1	SGL_2	SGL_3	SGL_4	RGS_1	RGS_2	RGS_3	RGS_4
2	0.001	0.002	0.002	0.001	0.001	0.002	0.002	0.001	0.002	0.002	0.001	0.001	0.002	0.001
3	0.002	0.002	0.001	0.002	0.002	0.002	0.001	0.002	0.002	0.002	0.002	0.001	0.001	0.002
5	0.003	0.001	0.002	0.001	0.001	0.002	0.002	0.001	0.001	0.001	0.001	0.001	0.001	0.001

2

Figure 1

Novel architecture with two routers

