Receive Satellite-Terrestrial Networks Data using Multi-Domain BGP Protocol Gateways

Tieshi Song[1], Zhanbo Liu[2]*
HongQi Hospital Affiliated to Mudanjiang Medical University, Mudanjiang Medical University,
Mudanjiang 157011, Heilongjiang, China[1]
Modern Education Technology Center, Mudanjiang Medical University, Mudanjiang 157011, Heilongjiang, China[2]

Abstract—**In terms of communication media, computer network technology has advanced significantly as a way of communication between devices. An Internet protocol called Border Gateway Protocol (BGP) is used to route traffic and share data between AS. But as of right now, BGP version 5 (BGP-5) has a fairly prevalent problem that degrades the performance of modern IP networks: "high convergence delay" when making routing changes. Since their formation at the start of the twenty-first century, satellite-terrestrial networks (STN) have drawn attention. Particularly in data centers and enterprise networks, this technology has greatly improved traffic control, administration, and monitoring. When adopting the STN paradigm, difficulties were discovered with providing administrative control, security, administration, and monitoring across domain borders. BGP-5 is used in a multi-domain STN to route traffic and communicate data across many domains or autonomous systems. Through fewer advertisement pathways, BGP-5 shields terrestrial networks from the high dynamics of satellites. Furthermore, a genuine network environment is constructed for authentic testing. According to the findings, BGP-5 can lower CPU consumption by 8.23% to 9.56% and bandwidth resource occupancy of the terrestrial network by 32.12% to 73.26%.**

Keywords—Internet of Things; satellite-terrestrial networks; multi-domain; BGP-5; protocol gateways

I. Introduction

The Internet is comprised of billions of interconnected network devices. It utilizes protocols that employ access and routing information to assist the flow of traffic [1, 2, 3]. Carrier and enterprise networks are referred to as autonomous systems (AS) which establish distinct domains within the Internet. Border Gateway Protocol version 5 (BGP-5) is a structured protocol used to route internet traffic and transmit access information between Autonomous Systems (ASs) [4, 5, 6]. Initially, the satellite network and the terrestrial network operated as distinct systems. Due to incompatibility, terrestrial routing protocols are not suitable for satellite networks [7]. Therefore, researchers primarily develop specialized routing systems for satellite networks. The study in [8] suggested a method for implementing IP routing within the satellite constellation network to enhance the dissemination of IP routing. Previous studies have suggested the implementation of routing strategies based on snapshots [9], [10]. The combined satellite-terrestrial networks primarily consist of the space network and the terrestrial network. The ground network consists of AS that are equipped with ground stations [11]. The network topology exhibits a high degree of stability and undergoes minimal changes during a specific timeframe. Satellite constellations largely dominate the space network [12]. The correlation between space and terrestrial networks will undergo a rapid transformation as satellites continue to migrate [13], [14]. The integrated satellite-terrestrial networks encounter a range of issues due to frequent changes in network structure [15]. Nevertheless, these systems treat the space network as a separate and self-contained system, distinct from the terrestrial network. Consequently, the space network lacks the routing information of the terrestrial network. When the ground station establishes communication with the satellite, it is necessary to enclose extra data packets, which leads to a significant increase in bandwidth usage [16]. BGP-5 is a decentralized protocol designed to facilitate the sharing and transfer of routing information between AS. BGP-5 utilizes the shortest path vector protocol [17]. Ongoing research is being conducted to address many challenges associated with BGP-5, such as enhancing performance, increasing robustness, improving security, and reducing routing update convergence delay [19], [20], [21]. The literature emphasizes the significance of BGP-5 in the operation of the Internet, as well as the challenges posed by the global nature of the Internet and the numerous legacy systems in place [22]. Efforts to modify or substitute BGP-5 have been hindered by these factors.

Researchers are currently exploring the application of the STN paradigm to rethink network architecture. Specifically, they are studying how this paradigm might enhance the management of inter-domain traffic flows [23]. STN enables the creation of the data plane by utilizing affordable "white label" boxes that serve as data transmission devices. The control plane is handed over to a novel category of network devices, referred to as controllers, which can oversee one or many data plane devices [24]. Fig. 1 shows the communication between the sensor and the web client through intermediaries for two sections a and b.

By embracing the STN paradigm, the process of implementing a network becomes more streamlined as the control logic may be modified to align with the initial network application and device specifications [25]. The STN architecture consists of three distinct layers: control, application, and infrastructure. Operational activities can be facilitated through the implementation of application programming interfaces (APIs). The APIs consist of the East, West, North, and South options. Researchers have emphasized the advantages of STN in multiple areas such as cloud

*Corresponding Author.

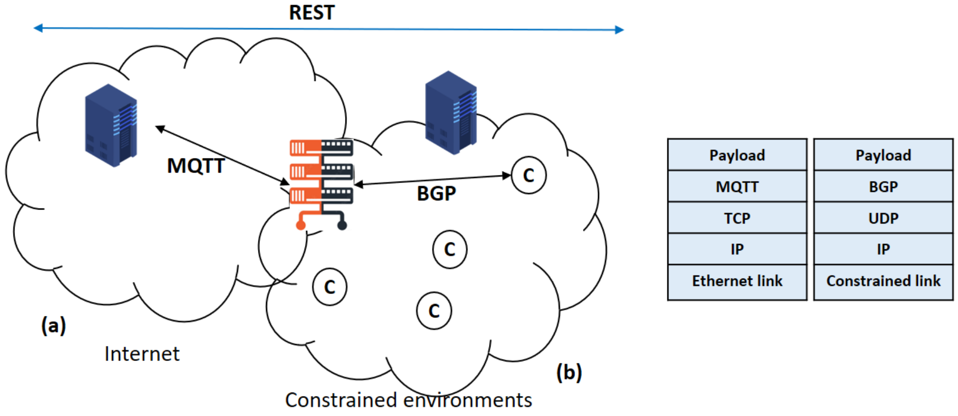
computing, the Internet of Things (IoT), and wireless networks. The writers in [26] have examined the difficulties and issues that can be addressed by the utilization of STN in wireless networks. The authors emphasize the benefits of the conventional OpenFlow protocol. STN can address difficulties related to traffic management, efficient load balancing, and optimal bandwidth use [27].

In networks that do not use STN, conventional networking methods employ intricate techniques due to the fact that the control plane and transmission plane are housed within a single device, allowing for manual updates to the device configuration. BGP-5 offers numerous benefits. Nevertheless, there are unresolved problems from the past. BGP-5 has undergone updates to address certain issues, and ongoing research is being conducted. In their study, the authors in study [28] proposed principles that attempt to reduce the occurrence of loops when utilizing BGP-5 and IGP. STN also offers dynamic programmability, which allows for the immediate deployment and updating of overlapping applications and services.

The primary objective of this paper is to investigate the impact of frequent alterations to links on the performance of terrestrial networks. Hence, a BGP-5, which is a lightweight version of the inter-domain routing protocol BGP, is suggested. BGP-5 introduces a backup route feature that utilizes BGP to enhance the route advertisement process and enhance the performance of the terrestrial network. The primary research contributions can be succinctly described as follows:

- Presently, STN technology lacks a universally accepted method for communication between controllers in a multi-domain network based on STN.
- The primary constraint of BGP-5 is the significant latency in achieving convergence.
- BGP-5 is designed to transmit routing and reachability information efficiently, but it has constraints that impact service delivery and the timely updating of routing tables.

The subsequent sections of the article are structured in the following manner. Section II provides an overview of prior research. The proposed approach is introduced in Section III. Section IV provide a description of the analysis, evaluation, and simulation. Section V, on the other hand, presents the conclusions and future activities.



Payload	Payload
MQTT	BGP
TCP	UDP
IP	IP
Ethernet link	Constrained link

Fig. 1. (a) The sensor and web client communicate using the M.QTT to BGP converter, allowing bidirectional data delivery. (b) The M.QTT protocol stack is located to the left of the proxy.

II. Related Work

Browsing is a prevalent example of Internet applications, in which users make requests for services offered by servers located on the Internet. In order to offer the service, data needs to be transmitted between the user's system and the server. The local network routing for the user is unable to establish a comprehensive data path [29]. Within the fundamental structure of the Internet, there exists a segment of the network that is under the jurisdiction of a single administrative authority. This segment, known as an autonomous system (AS), serves the purpose of offering local network assistance. Trade A comprehensive data route is built through the exchange of BGP routes. The absence of a centralized administration point and the existence of various Autonomous Systems (ASs) with intricate peer policies make security at this level of the Internet particularly difficult [30]. The article examines current methods for enhancing the security of the Border Gateway Protocol (BGP). The security techniques are classified into the following categories: The topics covered in the text are as follows: 1) encryption and authentication, 2) database management, 3) overlapping and clustering protocols, 4) penalty, and 5) data page testing. The strategies are evaluated comprehensively in an instructional fashion, and the limitations of the techniques are also succinctly presented. The coverage of specific published works is deliberately limited to ensure that the reader can easily understand the techniques. This survey serves as a foundation for assessing methods to comprehend the extent of published works and identifying the most effective paths for further investigation [31].

The advancement of computer network technology has greatly improved communication between devices through various communication methods. The BGP routing protocol uses a distinct method from the bandwidth to determine the ideal QoS value, as seen in study [32]. The test simulation findings indicate that employing bandwidths of 64 Kbps, 128 Kbps, and 256 Kbps, the QoS values for delay, jitter, packet handshake, and throughput in VoIP are consistently better than the average results obtained.

Network security is a crucial concept that encompasses internet applications, devices, and technologies. A confidential and secure network application is created by utilizing a mix of rules and parameters. Network security encompasses several concepts such as terms and conditions, rules, measures to prevent unwanted access, and protection against denial of service attacks. An effective network security system can enhance the protection of IT and banking applications, thereby mitigating the risk of theft by hackers. Under congested network conditions, numerous stability issues arise. Hence, it is imperative to employ sophisticated network security techniques in order to address the aforementioned constraints. A concise examination of different network security concerns and protocols was conducted in the study [33]. This article recommends articles on network security research in Internet applications. Furthermore, a comprehensive analysis is conducted on the benchmarks, and an evaluation of network security techniques from previous contributions is also undertaken. This survey specifically addresses different research issues and vulnerabilities that can assist researchers in implementing contemporary network security approaches on the Internet.

Recent research asserts that employing the Shortest-Path Tree Network (STN) methodology will be advantageous in resolving some Border Gateway Protocol (BGP) issues. STN can effectively administer BGP-based networks with minimal expense and complexity. Nevertheless, numerous scientific and operational challenges persist in this area of research. The primary objective of the research [34] is to ascertain the obstacles that BGP encounters in relation to the implementation of STN. The data indicate that the majority of researchers have prioritized enhancing the speed at which convergence occurs while overlooking crucial aspects like scalability and privacy.

Border Gateway Protocol (BGP) serves as the primary routing protocol for the Internet, acting as the cohesive force that links the several networks comprising the Internet. A border gateway protocol relay is created in [35] to receive border gateway protocol routing tables and updates from ISP core routers. Routers can utilize it to consistently exchange Border Gateway Protocol messages with adjacent routers. Furthermore, it has the capability to simulate reverting back to the identical routing table configuration at a preset interval when the routing tables are swapped. Therefore, it significantly enhances research on routing habits.

In order to ensure efficient and secure Internet access, it is crucial for the Border Gateway Protocol (BGP) to have the capability to promptly identify and prevent abnormal concurrency [36]. Although there has been an increase in the number of research conducted in the past decade to identify abnormalities in BGP, it remains necessary due to the emergence of novel and unusual behaviors exhibited by attackers and network misconfigurations. A novel BGP anomaly detection model consists of the following two primary components: The two main steps involved in this process are feature extraction and anomaly detection. Additional functionalities, such as "Statistical Features," "Higher Order Statistical Features," and "Improved." The Holo-entropy characteristics and "correlation features" are utilized to enhance the accuracy and dependability of recognition. Subsequently, the suggested DBN is implemented to identify the existence or nonexistence of an anomaly. Furthermore, a hybrid RHMFO optimization technique is employed to precisely adjust the DBN weights with the aim of enhancing the classification accuracy. The DBN result provides information regarding the presence or absence of network anomalies [37].

Studies have primarily investigated aggressive actions carried out by groups that specifically target AS. Border Gateway Protocol (BGP) hijacking has been responsible for numerous instances of interruptions and extensive eavesdropping. The researchers assessed potential attack strategies and put forth an attack strategy targeting AS connections through BGP hijacking. Their computer simulations provide a localized map of the AS (Autonomous System) topology using publicly available log data. By utilizing a topology map, it assesses the impact of the opposing group's actions.

III. Suggested Method

The details of a suggested method called STN are provided in this section. A network administrator commonly carries out the control functions of an AS on behalf of other organizations. An ISP is a prime example of an AS. Every AS must be allocated a distinct Autonomous System Number (ASN) which aids in the routing procedure when utilizing BGP-5. Normal circumstances prevent BGP-5 from being utilized as recommended.

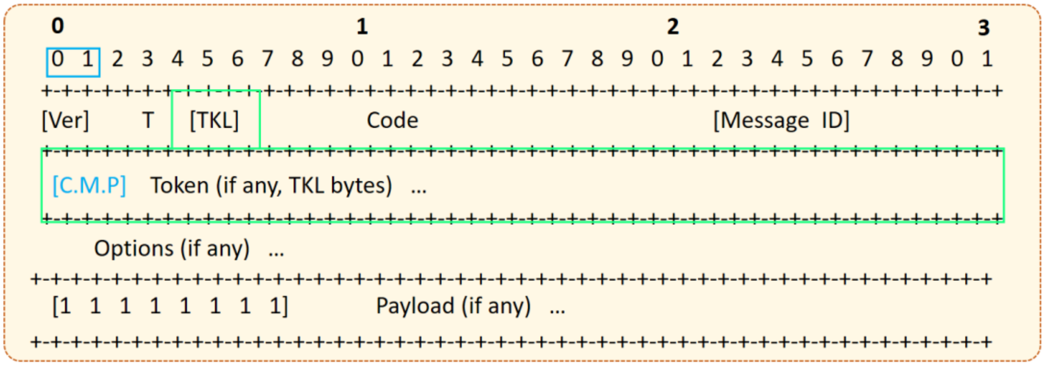


Fig. 2. Critical information scheduling in BGP-5 messages.

When someone is idle, they are waiting for a specific event to happen and for the information about that event to be communicated. Going forward, the term "sending" will be used instead of the forward technique. Here is the reasoning behind the node's change in status. When the status is set to 1, it signifies that the node is prepared to receive packets; the processing event generates the packets for transmission. The MAC layer acknowledges the receipt of the packet upon a status change of the network has effectively performed the duties described in the current document. a) BGP-5 facilitates the transmission of routing and reachability data through the use of Network Layer Reachability Information (NLRI) [3]. It is a resilient routing technology that is attributed to the advancement of Software-Defined Networks (SDNs). Like ForCes [23], BGP-5 offers network programmability support, enabling the application of encoded policies for network filtering and forwarding. SDN controllers have the capability to utilize BGP-5 protocol to transmit TCP packets. Essentially, BGP-5 serves as a facilitator of SDN by receiving routing instructions from the SDN controller and executing them across the centralized network [14]. b) The control of the reception process on sensor nodes is responsible for managing the timing and aggregation of messages, ensuring that each message adheres to its maximum allowable delay. The collected messages are then placed in the specified location. Furthermore, the utilization of the terms "packet" or "suitable size" in the context of aggregation signifies that the condition specified in Eq. (1) has been fulfilled.

$$\text{G(p)}\leq\text{CVR\_MAX\_P.LD\_SXL(OB)} \qquad (1)$$

The prioritization of Border Gateway Protocol (BGP-5) Control Management Protocol (CAP.MP) messages is divided into four distinct levels, as outlined in study [2].

$$0\leq \text{CAP.MP (S)} \leq 3 \qquad (2)$$

The priority level of three is the lowest, while zero is the highest. In order to ensure completeness, BGP-5 messages must have the storage location of the value as well. Peering refers to the establishment of a BGP-5 session between neighboring routers or gateways, when BGP-5 messages are exchanged across a Transmission Control Protocol (TCP) connection. The TCP connection creates the illusion of a transmission channel that consistently delivers a sequential stream of data, hence removing the need for BGP-5 to handle error repair or retransmission. The peering process entails a sequence of processes that necessitate the transmission of messages between peers in order to establish a BGP-5 peering session. Fig. 2 depicts the establishment of BGP-5 peering between two AS [27]. When two routers within the same Autonomous System (AS) establish a connection, it is known as internal BGP-5 or iBGP. In the same way, the process of peering can occur between peers situated in separate Autonomous Systems (ASs), which is known as external Border Gateway Protocol version 5 (eBGP5) in such cases. Peering can take place between edge or border routers, which are referred to as eBGP5 routers. iBGP peering is established by connecting intermediate routers. The primary distinctions between eBGP5 and iBGP arise during the path by Eq. (3).

$$\text{minimize}\sum\nolimits_{n_{i\text{€}N\backslash ER}}.\ |P_{n\ i}^{I}\ |+\sum\nolimits_{n_{i\text{€}N\backslash ER}}\ \ |P_{n\ i}^{O} \qquad (3)$$

The STN technique reduces the number of packets that are received by the nodes when they get information from the router's edge. This reduction includes the sum of the absolute values of $\sum_{m_{i\text{€}M\backslash FS}} |S_{p\ j}^{l}$ nodes. The maximum allowable time interval between receiving a packet (p) and sending it to node $|n_i$ is defined as [18]. The value representing time will be positive as specified by Eq. (4).

$$W_{m\ j}^{s} \leq 0 \qquad (4)$$

If the message is of the RST type, the maximum duration for which the node can retain the message is zero.

$$W_{m\ j}^{s}\text{=0}\quad \forall_{p}\in S_{p\ j}^{l},\forall_{p}\ \ \in S_{p\ j}^{l}\ \text{:type(p) = RST} \qquad (5)$$

The size of packets containing BGP-5 messages in the network layer (6LoWPAN) falls within the interval specified in Eq. (6), in accordance with the packet size limitations. Additionally, this layer has little packet overhead [26].

$$\forall_{P}\in P_{n\ i}^{O},\forall_{P}\in P_{n\ i}^{i}\ \forall_{P},\in P_{n\ i}^{s} \qquad (6)$$

Every stage of the design process will consider the restrictions indicated earlier. Specifically, the significance of $W_{m\ j}^{s}$ will be elucidated in relation to generated by the proposed technique is displayed below, accompanied by the corresponding pseudo-codes.

If the condition stated in criteria in Eq. (7) is satisfied, meaning that the receiving node takes a decision. The current package has not been given sufficient time to meet expectations [36]. Hence, the packet will be transmitted to the subsequent node with minimal anticipation on the part of that node.

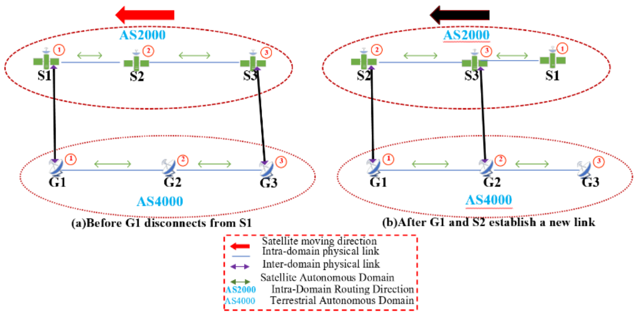
$$bs_{n\ i}^{p} = 1\text{⩘Dst×(p)}\neq n_j\wedge(CMP(P) = 0\vee \qquad (7)$$

As stated in reference [16], the advocates of STN leveraged the utilization of OpenFlow to segregate the data and control layers inside a network. Network operators have embraced the STN design, in part, because of its additional advantages such as programmability and operational agility.

$$bs_{n\ i}^{p} = 1\text{⩘Dst× (p)}\neq n_j\wedge(CMP(P) = 1\vee \qquad (8)$$

A. Routing from Satellites to Earth: a Stability Issue

Our study is inspired by the spatial-terrestrial network architecture shown in Fig. 3. Each satellite and ground station in the Autonomous System (AS) 2000 and AS 4000, respectively, has an IPv6 accessible network assigned to it. By using BGP and along with routing updates, they can advertise route prefix information over the link.


AS2000
S1
S2
S3
G1
G2
G3
AS4000
1
2
3
AS2000
S2
S3
S1
G1
G2
G3
AS4000
1
2
3
Satellite moving direction
Intra-domain physical link
Inter-domain physical link
Satellite Autonomous Domain
AS2000 Intra-Domain Routing Direction
AS4000 Terrestrial Autonomous Domain

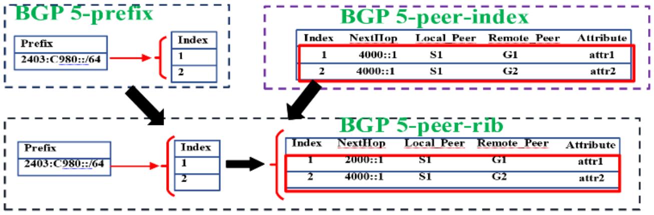
(a)Before G1 disconnects from S1

(b)After G1 and S2 establish a new link

Fig. 3. The design of networks that combine satellite and ground service.

This process is illustrated in Fig. 3(a). When S1 flies lower than G1, the BGP peer connection breaks down, and the two no longer exchange routing data (Fig. 3(b)). The S2 satellite is now circling the Earth, directly over the G1 base station. Something new happens when G1 and S2 become neighbors. The routing domain routes of both G1 and S2 are advertised to each other.

Step two involves repositioning satellite S1 to the location shown in Fig. 3(a). The inter-domain neighbor relationship is restored and routing information is exchanged between S1 and G1. Nevertheless, the majority of the routing details being promoted at the moment have previously been promoted in past messages. Both ends of the connection are drained of precious bandwidth resources by a flood of route ads. Hence, it is important to think about ways to decrease bandwidth consumption by reducing the number of route ads when the BGP neighbor connection is re-established.



Prefix
2403:C980::/64

Index
1
2

Index	NextHop	Local_Peer	Remote_Peer	Attribute
1	4000::1	S1	G1	attr1
2	4000::1	S1	G2	attr2

Prefix
2403:C980::/64

Index
1
2

Index	NextHop	Local_Peer	Remote_Peer	Attribute
1	2000::1	S1	G1	attr1
2	4000::1	S1	G2	attr2

Fig. 4. The redundant S1 satellite routing data.

B. Design Information of the BGP-5

Border routers using BGP-5 do not re-advertise route prefixes to each other after re-establishing a neighbor connection, in contrast to ordinary BGP that does so at every neighbor relationship establishment. When backup routing information is enabled, both communication parties will be notified of any updates to the routing.

1) Collect contingency routing data: Both the BGP PEER RUB and the BGP PEER INDEX tables are maintained by BGP-5 to ensure the safety of routing information. Its purpose is to capture the real-time routing data that this router receives and transmits from other border routers in the autonomous system. Consider satellite S1 (Fig. 4) for the sake of simplicity of explanation. As S1 keeps moving, it connects with ground stations G1 and G2, forming neighbor associations. Fig. 4 illustrates the process of updating the inter-domain topology routing table when satellite node S1 receives routing messages from several ground stations and records the prefix and peer information.

During the waiting period, the following tasks are performed: The minimum value between the current WT and 9 is utilized.

$$\text{WT}\leftarrow \min\{\text{WT}, W_{n\ i}^{p}\} \tag{9}$$

This indicates that the message received is composed of many sub-packets, with each sub-packet serving as a message for the UDP/BGP-5 layer.

$$\text{If } bs_{n\ i}^{p}\text{=1 then } \forall\ sub_j^p\ \in \text{S if Dst}(sub_j^p)\text{=}n_i$$

$$\text{,Dis\_join}(sub_j^p\text{,S}) \tag{10}$$

Therefore, the lack of transmission, as seen in the status diagram of Fig. 5, is of minimal importance. The importance of the packet generated by the node for this purpose is considered negligible.

$$\text{(MDW-CanWait(CUL-Max-PDU(}P_g\text{)-L}\times\text{(Q.B)-}\Delta\text{,}W_{n\ i}^{p}\text{)=0)} \tag{11}$$

Algorithm 1 provides a clear description of the procedure for moving from stages 7 to 8.

Algorithm 1: Pseudo-code and the current segmentation situation

```
Algorithm Dis_join
Input: Packet s
Output: Void
Note: The Dis_join method extracts sub-packets from the input and
calculates the next state.
 if ($bs_{n\ i}^{p}$ =0) then
 for each $sub_j^p$ in S do
 $p_j$= Extract($sub_j^p$,) // Extract sub-packet subjp from S
if Dst($s_k$) = nk and nk ≠ n_i then
// Next hop grouping and joining for sj and sk
Next hop grouping and joining (sj, $s_k$)
else if Dst($s_k$) = n_i then
// Call the Receive function for s_j
call Receive($s_k$)
state ← Receive // Update state end if end for
// Call the Forward function for $s_k$call Forward($s_k$)
state ← Forward
// Update state
end if
return
```

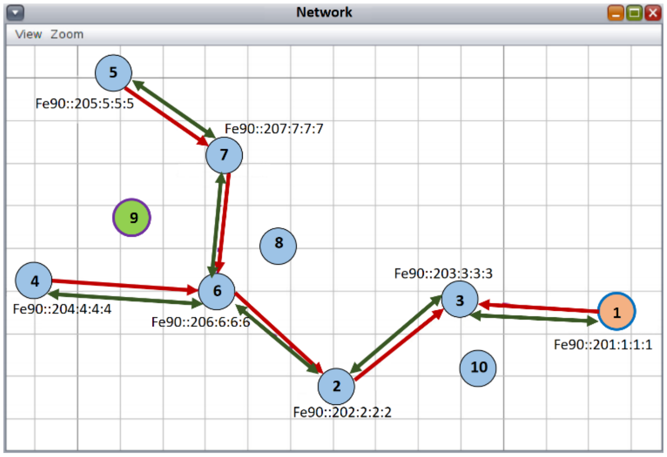


Fig. 5. Aggregated information transfer that has undergone numerous steps of consolidation.

IV. Discussion and Evaluation

In this section, we construct a miniature operational network environment to conduct practical tests and assess the efficiency of BGP-5. Fig. 6 displays the configuration of the test platform. The platform consists of several routers equipped with Quagga routing software. The router nodes are interconnected using a 3000 Mb Ethernet connection, and the time it takes for data to travel between the nodes is set at 50 ms.

In order to replicate the changes in the network structure of the space-earth fusion network.

Both networks utilize the CTP protocol [3] for packet transmission and forwarding on each node. We derive the whole routing topology for data collecting and calculate the average ETX value of each link using C1 and C2 packet types. With default parameters for ZigBee transmissions. These settings include a sleep interval of 600 ms, a radio-on window of 11 ms, and a packet retransmission threshold of M = 4. The power levels of sensor nodes are configured as follows: the transmit power level (Ptx) is set to 40 milliwatts, the receive power level (Prx) is set to 10 milliwatts, and the idle power level (Pidle) is set to 0.007 milliwatts. Each test had a period of one hour, and the topology was modified four times. Different amounts of routing information are sent from the ground station to the satellite nodes in each transmission. To capture the simulation results, you need to install the tcpd.ump software on the G1 device. After that, you can use the iftop command to measure the amount of traffic transmitted across the interface.

A. *The Success Rate in Decreasing Outgoing Packets (PS_s^M)*

This article employs four primary metrics to assess the effectiveness of BGP-5 versus regular BGP: Network traffic consumption refers to the total amount of data transmitted by the ground network in the form of packets throughout the test time. The term "message overhead" pertains to the overall quantity of routing messages that were publicized by the terrestrial network throughout the duration of the test time.

$$PS_t^M = \frac{G_s^M}{Y_s^M} \times 200 \tag{17}$$

The calculation of G_s^M is done by referring to Eq. (18). The numerical value is also represented by the notation Y_s^M. From the beginning of the network until its evaluation at the current moment, the total number of packets received or created using the BGP approach for all sensor rounds (excluding the edge router) is 19 (inclusive).

$$M_t^N = \sum_{m_i \in N \backslash RE} |P_n^I{}_i| + \sum_{m_i \in N \backslash RE} \tag{18}$$

$$X_t^N = \sum_{m_i \in N \backslash RE} |PS_t^M| + \sum_{m_i \in N \backslash RE} |PS_t^n| \tag{19}$$

B. *Degree to which Traffic is Reduced Differs According*

It is necessary to calculate these metrics for every procedure executed by the gateway in order to obtain the duration of transmission and the dependability of the combined data packets. Two main causes of traffic jams are application consumption and performance. Table I shows the physical layer packet structure.

TABLE I. PHYSICAL LAYER PACKET STRUCTURE OF EEE802.16.5 VERSION 2012

PUDP arrangement	
PDUS	Footer of PUDP
packet drop ratio	queue for forwarding, the mean waiting time
inside 128_bytes	5 bytes to 2 byte

We have documented the network lifetime under different packet generation rates to investigate the effect of traffic dynamics on the performance of the gateway deployment. The majority of the time, our gateway implementation can deliver satisfactory performance. To no one's surprise, a higher packet creation rate per node will reduce the network lifetime. It may go against our previous results, but we also observe that the lifetime under a large k is less than the lifetime under a small k when the packet generation rate is relatively high. Our investigation of the effect of k on network performance aims to shed light on the rationale underlying this phenomena.

$$TRS_t^N = M_s^N \times M_t^N \text{ b}_{\text{yte}} \tag{20}$$

Among the packets received by v_i, only M_t^N are selected for placement in the forwarding queue, while the rest are discarded. This is represented by TRS_t^N. After each packet in the preceding queue has been delivered, the newly received packet is transmitted in the first-in, first-out (FIFO) forwarding queue. The average amount of time a packet spends waiting in the forwarding queue in Eq. (21).

$$\mathrm{TRS}_t^{n_i} = \mathrm{N}_t^{m_i} \times \text{-} \ \mathrm{N}_t^{m_i} \text{ b}_{\text{yte}} \tag{21}$$

When the forwarding queue reaches its maximum capacity, the gateway will discard any additional packets. To simplify, we will focus on the performance following the overflow of the forwarding queue. The reliability $\mathrm{N}_t^{m_i}$ at the BN-IoT side, which represents the chance of gateway vi successfully forwarding an incoming packet to BS, may be expressed as Eq. (22):

$$\mathrm{TRS}_1^N = \frac{\mathrm{TRS}_t^M}{t} \text{ byte/s} \tag{22}$$

C. *Amount of Reduction in Energy Consumption According to Energy Consumption ($TRS_{m_i}^{m_J}$)*

Sensor nodes deplete energy through the activities of communication, sensing, storage, and data processing. To ascertain the energy consumption linked to the transmission of a solitary byte inside a network. Table II shows the recently received packets MAC layer. Out of all these operations, communication is usually the primary consumer of energy. Each sensor node has three distinct modes: 1) transmission mode, 2) reception mode, and 3) idle mode.

TABLE II. THE RECENTLY RECEIVED PACKET'S MAC LAYER AUTHENTICATION, IEEE802.16.5: 2012 EDITION

	packet loss rate of acknowledge	
complete dependability Verify the housing	field for gateway waiting times for sequence numbers	control of the frame
3 byte	2 byte	3 byte

The energy consumption rate En_{send}^1 of a sensor node E_s can be expressed as in Eq. (23):

$$E^1 = E_{send}^1 + E_{Receive}^1 \tag{23}$$

Every gateway has a First-In-First-Out (FIFO) forwarding queue for all outgoing packets. This queue stores both the packets created by the gateway itself and the packets received from other nodes. The energy required to transmit one byte from node i to a nearby node in a single step is represented as

En_{send}^{1} , while the energy needed for node j to receive the same byte is represented as En_{reciv}^{1} .To ensure efficient forwarding of incoming packets to the base station (BS), we utilize the data aggregation algorithm [9] for the gateways. In this paradigm, the gateway only carries out data transfer when the number of combined packets reaches a specified aggregation number, ki. Prior to data transmission, gateways may need to perform preliminary operations to calculate the transporting by Eq. (24), which quantifies the degree of decrease in energy.

$$\mathrm{TRS}_{m_i}^{m_J}=(E^{1}\times\ \mathrm{H}_{n_i}^{n_J} \times\mathrm{RTR}_{t}^{n_i}) -(\varepsilon \times \mathrm{M}_{t}^{n_i}) \tag{24}$$

The variable ps,l reflects The likelihood of a successful unicast transmission across a network a certain link l, which is dependent on the MAC protocol. The symbol $\mathrm{TRS}_{\mathrm{t}}^{\mathrm{n_i}}$ denotes the rate at which the number of sent bytes by the node decreases up to time t. $\mathrm{N}_{t}^{m_i}$ represents the distance between node m_{i} to $\mathrm{m_j}$, and 3 signifies the average computational capacity. By employing Eq. (24), it is possible to calculate the amount of energy saved over the entire network, as the User Equipment (UE) does not need to listen to the paging messages. The User Equipment (UE) will initiate the Random Access (RA) operation just when it requires transmitting a packet to the Base Station (BS).

$$RTR_{n_i}^{n_J} \cong 0/24 \times \mathrm{H}_{n_i}^{n_J}\times\mathrm{RTR}_{t}^{n_i} \tag{25}$$

Therefore, the computational burden is ignored due to the effectiveness of the algorithms used in the proposed method. Therefore, Eq. (25) can be simplified. It is possible to accurately calculate the amount of energy saved when transmitting a single bit. The architecture of the intended network's multi-step network may be observed in Fig. 6, where nodes 9, 10, and 11 are not operational. Furthermore, it is important to highlight that nodes 6 and 4 have a vital function in enabling the transfer of packets between node 32 and the edge router.

The events linked to these grams have a byte value that falls between the range of 4 to 12. Table III displays a comprehensive summary of the main characteristics. The simulated network, together with the characteristics associated with the suggested methodology.

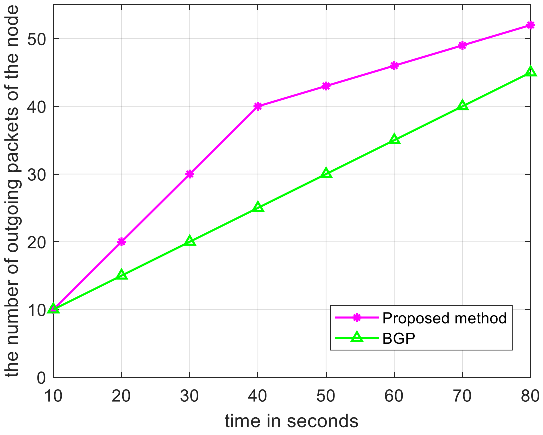


Fig. 6. The number of output packets generated by the second node within a 600-second timeframe distinguishes the BGP method from the suggested methodology.

TABLE III. SIMULATION PARAMETERS

Measure	Amount
The size of the application layer packets that are created	18 to 26 bytes
Packet size at the network layer in LoWPAN6.	43 to 56 bytes
Package size in the Mac layer refers to the size of the data packets that are transmitted and received at the Media Access Control (MAC) layer of a network protocol.	69 to 81 bytes
The aggregate number of packets generated across all nodes during the experiment.	216 packages
The time it takes for the node to create a packet	526 to 5124 years
Duration of the simulation	500 seconds
Packet priority (CMP)	4 (Notes with standard priority)
The Maximum Allowed Time (MAD)	5 seconds
Public-Private Partnership for Vaccines and Immunization	0.89

We may ensure high performance without compromising transmission reliabilities and latencies. The aggregate number k for all deployed gateways is set to 3. Fig. 6 presents the optimization findings, where "G = 1" represents the initial performance with an 802.16.5 sink node. Our analysis reveals that our gateway implementation significantly enhances the longevity of the network. implementing a single gateway extends the lifetime of the network by 39.1% to 82.4%, while implementing six gateways extends it by 535.02% to 703.8%. Fig. 7 illustrates the results achieved by implementing the results compared to the BGP method, while keeping the settings the same. The given information displays a data diagram that shows the transfer of packets starting at node 3, as shown in Fig. 7. The red figure represents the normal operation.

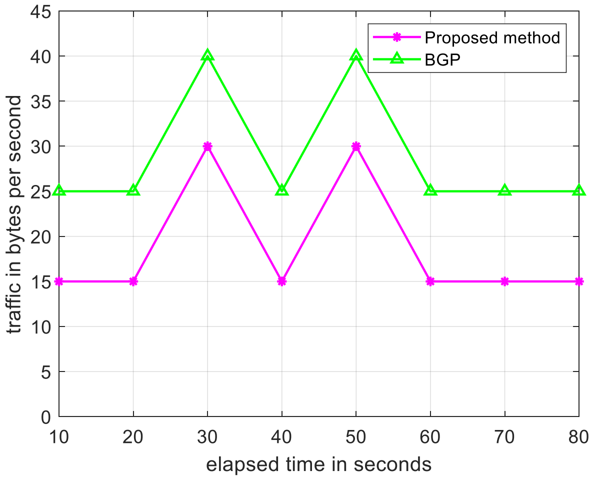


Fig. 7. The deviation, calculated over a duration of 500 seconds, between the BGP technique and the proposed method for the outgoing traffic of node number 3.

V. CONCLUSION

This strategy is an innovative initiative designed to reduce the negative effects of message transmission, particularly in terms of traffic congestion and energy consumption. Using Border Gateway Protocols (BGP) has been proposed for multitime networks that depend on the Wireless Personal Area Network (WPAN) protocol stack. The protocol stack being discussed is known for its complex and extensive features and functionalities across multiple tiers. When it comes to monitoring, the focus is on the lower tiers of the network layer, particularly in regards to decision-making about waiting, as controlled by the decision-making aspect of waiting (DMW).

Additional research and analysis have the potential to reduce the significant computational load caused by the User Datagram Protocol (UDP) layer. Since the UDP packets are intended to include CoAP messages within the router layer, it is possible to remove the destination port segment and header field when aggregating network traffic. This elimination might take place within the network layer of the receiving node before transferring the packet to the upper layer protocol (UDP) for reconstruction. Additionally, considering the different levels of importance of client requests and the ability to hide and set time limits for answer messages in the BGP protocol, it is feasible to create a more appropriate categorization and management layer. One way to achieve this is by incorporating a request priority queue into the router. This queue helps in the creation and handling of requests. This concerns the handling of requests received by the Low-Rate Wireless Personal Area Network (LR-WPAN) using the BGP protocol stack, and the consequent creation of answers. Moreover, through the recognition of patterns in network references, it is possible to obtain the required information before receiving the request by using the models. The person analyzed time series data and applied network concepts using the WAPN protocol stack in the fields of health and security.

Funding

This work was supported by Mudanjiang Municipal Bureau of Science and Technology (Guidance) Project (Grant No.: HT2022NS107).

References

[1] H. Alqahtani, L. Niranjan, P. Parthasarathy, and A. Mubarakali, “Modified power line system-based energy efficient routing protocol to improve network life time in 5G networks,” Computers and Electrical Engineering, vol. 106, p. 108564, 2023.

[2] F. Ouakasse and S. Rakrak, “A comparative study of MQTT and COAP application layer protocols via. performances evaluation,” Journal of Engineering and Applied Sciences, vol. 13, no. 15, pp. 6053–6061, 2018.

[3] M. F. KM, N. Santhiyakumari, and M. Suganthi, “Augmentation of Intelligent Agent for Multiple Access Protocols in Wireless Sensor Networks,” in 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), IEEE, 2022, pp. 1361–1367.

[4] X. Zhao, S. S. Band, S. Elnaffar, M. Sookhak, A. Mosavi, and E. Salwana, “The implementation of border gateway protocol using software-defined networks: A systematic literature review,” IEEE Access, vol. 9, pp. 112596–112606, 2021.

[5] K. H. Manguri and S. M. Omer, “SDN for IoT environment: a survey and research challenges,” in ITM web of conferences, EDP Sciences, 2022, p. 01005.

[6] Li, S., Wu, Q., & Wang, R. (2024). Dynamic Discrete Topology Design and Routing for Satellite-Terrestrial Integrated Networks. IEEE/ACM Transactions on Networking.

[7] Zhang, L., Hu, S., Trik, M., Liang, S., & Li, D. (2024). M2M communication performance for a noisy channel based on latency-aware source-based LTE network measurements. Alexandria Engineering Journal, 99, 47-63.

[8] Khosravi, M., Trik, M., & Ansari, A. (2024). Diagnosis and classification of disturbances in the power distribution network by phasor measurement unit based on fuzzy intelligent system. The Journal of Engineering, 2024(1), e12322.

[9] Liao, Y., Tang, Z., Gao, K., & Trik, M. (2024). Optimization of resources in intelligent electronic health systems based on Internet of Things to predict heart diseases via artificial neural network. Heliyon.

[10] Li, Y., Wang, H., & Trik, M. (2024). Design and simulation of a new current mirror circuit with low power consumption and high performance and output impedance. Analog Integrated Circuits and Signal Processing, 1-13.

[11] Saidabad, M. Y., Hassanzadeh, H., Ebrahimi, S. H. S., Khezri, E., Rahimi, M. R., & Trik, M. (2024). An efficient approach for multi-label classification based on Advanced Kernel-Based Learning System. Intelligent Systems with Applications, 21, 200332.

[12] Wang, G., Wu, J., & Trik, M. (2023). A novel approach to reduce video traffic based on understanding user demand and D2D communication in 5G networks. IETE Journal of Research, 1-17.

[13] J. Maktoubian and K. Ansari, “An IoT architecture for preventive maintenance of medical devices in healthcare organizations,” Health Technol (Berl), vol. 9, pp. 233–243, 2019.

[14] Zhang, H., Zou, Q., Ju, Y., Song, C., & Chen, D. (2022). Distance-based support vector machine to predict DNA N6-methyladenine modification. Current Bioinformatics, 17(5), 473-482.

[15] Asghari, A., Zoraghchian, A. A., & Trik, M. (2014). Presentation of an algorithm configuration for network-on-chip architecture with reconfiguration ability. International Journal of Electronics Communication and Computer Engineering (IJECCE), 5(5), 124-136.

[16] Khezri, E., Zeinali, E., & Sargolzaey, H. (2023). SGHRP: Secure Greedy Highway Routing Protocol with authentication and increased privacy in vehicular ad hoc networks. Plos one, 18(4), e0282031.

[17] Khalafi, M., & Boob, D. (2023, July). Accelerated primal-dual methods for convex-strongly-concave saddle point problems. In International Conference on Machine Learning (pp. 16250-16270). PMLR.

[18] J. Sun, Y. Zhang, and M. Trik, “PBPHS: a profile-based predictive handover strategy for 5G networks,” Cybern Syst, pp. 1–22, 2022.

[19] Zhu, J., Hu, C., Khezri, E., & Ghazali, M. M. M. (2024). Edge intelligence-assisted animation design with large models: a survey. Journal of Cloud Computing, 13(1), 48.

[20] Cao, C., Wang, J., Kwok, D., Cui, F., Zhang, Z., Zhao, D., ... & Zou, Q. (2022). webTWAS: a resource for disease candidate susceptibility genes identified by transcriptome-wide association study. Nucleic acids research, 50(D1), D1123-D1130.

[21] Ding, X., Yao, R., & Khezri, E. (2023). An efficient algorithm for optimal route node sensing in smart tourism Urban traffic based on priority constraints. Wireless Networks, 1-18.

[22] M. Trik, H. Akhavan, A. M. Bidgoli, A. M. N. G. Molk, H. Vashani, and S. P. Mozaffari, “A new adaptive selection strategy for reducing latency in networks on chip,” Integration, vol. 89, pp. 9–24, 2023.

[23] Xiao, L., Cao, Y., Gai, Y., Khezri, E., Liu, J., & Yang, M. (2023). Recognizing sports activities from video frames using deformable convolution and adaptive multiscale features. Journal of Cloud Computing, 12(1), 167.

[24] D. K. Gupta and D. Pathak, “A Review on Load Balancing in Data Routing Of Wireless Sensor Networks,” Webology (ISSN: 1735-188X), vol. 18, no. 6, 2021.

[25] S. K. Singh and B. Mondal, “A fuzzy-based clustering and data collection for internet of things based wireless sensor networks,” in 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), IEEE, 2021, pp. 303–308.

[26] M. Jutila, “An adaptive edge router enabling internet of things,” IEEE Internet Things J, vol. 3, no. 6, pp. 1061–1069, 2016.

[27] M. Trik, A. M. N. G. Molk, F. Ghasemi, and P. Pouryeganeh, “A hybrid selection strategy based on traffic analysis for improving performance in networks on chip,” J Sens, vol. 2022, 2022.

[28] F. Ouakasse and S. Rakrak, “A comparative study of MQTT and COAP application layer protocols via. performances evaluation,” Journal of Engineering and Applied Sciences, vol. 13, no. 15, pp. 6053–6061, 2018.

[29] Esmaeili, N., & Bamdad Soofi, J. (2022). Expounding the knowledge conversion processes within the occupational safety and health management system (OSH-MS) using concept mapping. International Journal of Occupational Safety and Ergonomics, 28(2), 1000-1015.

[30] Z. U. Khan et al., "A comprehensive survey of energy-efficient MAC and routing protocols for underwater wireless sensor networks," Electronics (Basel), vol. 11, no. 19, p. 3015, 2022.

[31] B. HassanVandi, R. Kurdi, and M. Trik, "Applying a modified triple modular redundancy mechanism to enhance the reliability in software-defined network," Mapta Journal of Electrical and Computer Engineering (MJECE), vol. 3, no. 1, pp. 10–16, 2021.

[32] Khezri, E., Yahya, R. O., Hassanzadeh, H., Mohaidat, M., Ahmadi, S., & Trik, M. (2024). DLJSF: Data-Locality Aware Job Scheduling IoT tasks in fog-cloud computing environments. Results in Engineering, 21, 101780.

[33] Z. Wang, Z. Jin, Z. Yang, W. Zhao, and M. Trik, "Increasing efficiency for routing in internet of things using binary gray wolf optimization and fuzzy logic," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 9, p. 101732, 2023.

[34] M. Samiei, A. Hassani, S. Sarspy, I. E. Komari, M. Trik, and F. Hassanpour, "Classification of skin cancer stages using a AHP fuzzy technique within the context of big data healthcare," J Cancer Res Clin Oncol, pp. 1–15, 2023.

[35] Hedayati, S., Maleki, N., Olsson, T., Ahlgren, F., Seyednezhad, M., & Berahmand, K. (2023). MapReduce scheduling algorithms in Hadoop: a systematic study. Journal of Cloud Computing, 12(1), 143.

[36] Muniyappan, Y., Thiruvalar, N., & Kayathri, K. (2024, June). Implementation of BGP with similar and distinct AS numbers in MPLS VPN networks. In AIP Conference Proceedings (Vol. 3112, No. 1). AIP Publishing.

[37] Silalahi, L. M., Amaada, V., Budiyanto, S., Simanjuntak, I. U. V., & Rochendi, A. D. (2024). Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company. International Journal of Electronics and Telecommunications, 70.