Heliyon 10 (2024) e31625

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Receive wireless sensor data through IoT gateway using web client based on border gateway protocol

Meng Yan

School of Electrical Information, Changchun Guanghua University, Changchun, Jilin, 130000, China

ARTICLE INFO

Keywords:
Internet of things
BGP multistep
Energy consumption
Traffic reduction
Aggregation

ABSTRACT

One of the significant topics in the field of the Internet of Things (IoT) pertains to the interaction and information sharing among people. The utilization of the Border Gateway Protocol (BGP) stack enhances the integration of web protocols and sensor networks, leading to greater accessibility. However, the BGP protocol stack introduces substantial overhead to messages transmitted at each layer, resulting in increased data overhead and energy consumption in networks by several orders of magnitude. This paper proposes a method to reduce the overhead on small and medium-sized packets. In multi-temporal networks utilizing BGP, scheduling and aggregating BGP packets at sensor nodes help achieve specific objectives. Various research methodologies and measures are employed to facilitate this, including request classification, BGP response prioritization within the network, determination of maximum acceptable delay, and overall network management. Synchronization and temporal integration of received messages at sensor nodes are performed, considering the maximum allowable delay for each message and the availability of the destination to process the accumulated messages. The evaluation results of the proposed method demonstrate a significant reduction in energy consumption and network traffic, particularly in monitoring applications within multi-stage networks. The protocol stack used is derived from the BGP standard.

1. Introduction

Wireless networks characterized by low power and significant loss include routers that face limitations in terms of memory, processing capability, and power source, similar to the nodes they are interconnected with [1]. Some communication aspects of the system include low data rates, communication instability, and a high rate of communication and information loss [2–4]. The Internet Engineering Task Force (IETF) has developed a standardized protocol called LoWPAN, which facilitates the utilization of IPv6 on wireless networks with minimal data loss [5,6]. The utilization of this protocol enables the implementation of Low-Power and Lossy Networks using IPv6, encompassing networks constructed on the IEEE 802.15.4 standard [7]. Among the benefits of the LLN-based network is its capacity to incorporate traditional web architecture services into its application layer [8,9]. This integration facilitates connectivity with the internet and the web, enabling seamless communication between objects through web protocols [10]. The term “Web of Things (WoT)" is commonly used to refer to this concept [11]. Within the domain of the IoT, a diverse range of applications is accessible, wherein wireless sensors can establish connectivity through the internet [12]. Several applications can be identified, such as the utilization of data from body-attached sensors for remote patient condition monitoring and the web-based control of wireless sensor arrays by human operators [13,14]. Nevertheless, traditional web protocols such as Message Queuing

E-mail address: yanmeng_192210@sina.com.

https://doi.org/10.1016/j.heliyon.2024.e31625
Received 13 January 2024; Received in revised form 17 May 2024; Accepted 20 May 2024
Available online 21 May 2024

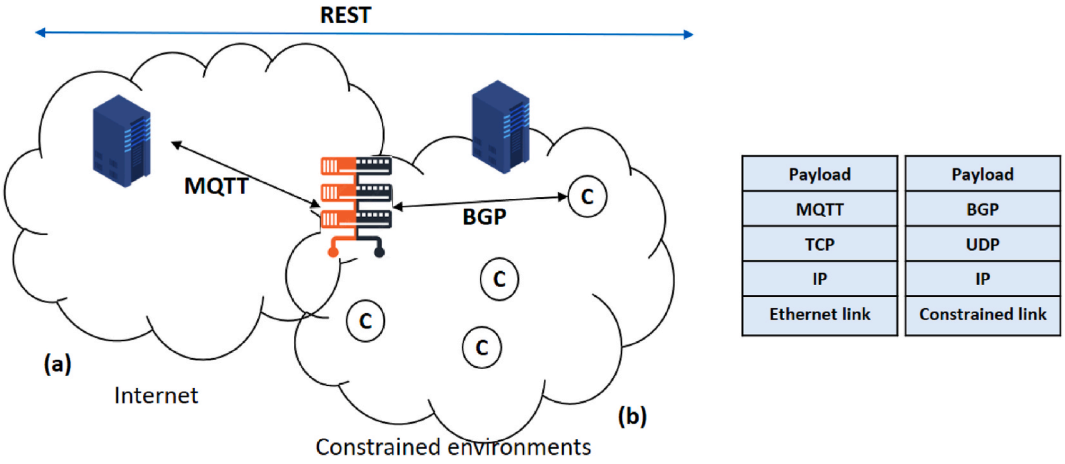
Telemetry Transport (MQTT) are not specifically engineered to operate efficiently on devices that possess limited quantities of random-access memory (RAM) and processing capabilities [15]. The MQTT protocol (see Fig. 1) is dependent on TCP connections that are both secure and dependable. Fig. 1a shows how data transmission between the web client and the sensor is made possible by the MQTT to BGP converter acting as an intermediary. Fig. 1b shows how the BGP protocol stack passes through the proxy on the right side, while the MQTT protocol stack is positioned on the left. However, it is important to note that network communications do not always exhibit a high level of reliability [16]. Due to their reliance on battery power, limited memory capacity, and constrained computational capabilities, the integration of web protocols with wireless sensors would incur significant costs. Consequently, the IETF introduced a streamlined version of MQTT called BGP. BGP encompasses an Internet of Things gateway, a unique web transport protocol intended for use on tiny networks and nodes. Additionally, it incorporates a range of hardware, software, and access controls that function as an intermediary between the Internet and sensor networks [17–19].

Furthermore, a proxy refers to a software component that functions as an intermediary for client requests [20,21]. Its role involves accepting these requests and subsequently searching the servers to locate the necessary resources for their fulfillment. Networks operating in the application layer that utilizes the BGP possess the capability to establish communication with networks employing MQTT due to the numerous resemblances shared by the BGP and MQTT protocols [22–24]. One possible approach to accomplish this is by employing a simple transit proxy that facilitates the translation of BGP to MQTT and vice versa. The task has been completed. A pass-through proxy is implemented on the IoT gateway to facilitate the conversion between the MQTT and BGP protocols [25].

The research presented in the paper holds significant consequences for both society and science. From a societal perspective, the optimization of BGP utilization in IoT networks leads to tangible benefits such as reduced energy consumption and improved network performance. This has implications for various IoT applications, including remote patient monitoring and environmental sensing, where energy efficiency is crucial for long-term sustainability. Moreover, by enhancing the scalability of IoT systems, the research contributes to the broader adoption of IoT technology, potentially revolutionizing various industries and improving quality of life. From a scientific standpoint, the method proposed in the paper advances our understanding of network optimization techniques in resource-constrained environments. By integrating scheduling and aggregation strategies, the research offers novel insights into mitigating overhead and energy consumption in multi-temporal networks, paving the way for further advancements in IoT infrastructure design and implementation.

While previous studies have explored methods for connectivity and communication in IoT systems, there is a significant lack of comprehensive strategies to address the specific challenges posed by combining BGP with sensor networks. The importance of this gap lies in the increasing prevalence of IoT applications and the need for efficient and sustainable network solutions. By proposing a method to reduce overhead and energy consumption in multi-temporal networks using BGP, this research addresses a critical need in this field and provides a new approach to optimize network performance and increase the scalability of IoT systems. The paper distinguishes itself from previous related studies by focusing specifically on optimizing BGP utilization in IoT networks to reduce overhead and energy consumption. While existing research has explored connectivity and communication protocols in IoT systems, the proposed method offers a unique approach to address the challenges posed by integrating BGP with sensor networks. Previous studies may have touched upon aspects of network optimization or energy efficiency in IoT, but none have comprehensively tackled the specific issues addressed in this research. By emphasizing the importance of reducing overhead and energy consumption in multi-temporal networks using BGP, the paper contributes a novel perspective to the field, offering practical solutions to enhance the performance and sustainability of IoT systems.

The research presented herein offers several advantages for optimizing the utilization of BGP in IoT networks. By incorporating scheduling and aggregation techniques within sensor nodes, this methodology effectively mitigates data overhead and energy



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

Fig. 1. (a) Communication between the sensor and the web client occurs through the intermediary of the MQTT to BGP converter, enabling data transmission in both directions, (b) MQTT protocol stack is situated on the left side of the proxy, while the BGP protocol stack is positioned on the right side of the proxy when it passes through.

consumption, particularly for small to medium-sized packets. This approach finds support in scientific literature such as [18], which demonstrates the efficacy of the BGP routing protocol in attaining optimal quality of service (QoS) across various bandwidths. Moreover, by leveraging the principles of Representational State Transfer (REST) architecture, this approach ensures efficient communication while accommodating the constraints imposed by sensor networks, such as packet size and bandwidth limitations. The adoption of this methodology is warranted by its capacity to tackle specific challenges inherent in Internet of Things systems, furnishing a pragmatic solution to enhance network efficiency and scalability. The primary contributions of the authors in this study can be encapsulated as follows.

- Introduction of CSAM (Critical Information Scheduling and Aggregation Method) aimed at minimizing the overhead associated with small and medium data packets in multi-hop networks employing the BGP stack. This method entails scheduling and aggregating BGP packets within sensor nodes to curtail energy consumption and network congestion.
- Introduction of techniques for categorizing BGP requests and responses based on their transmission priority within the network. This prioritization facilitates effective packet management and reduces latency in critical data delivery.
- Presentation of methods for managing message scheduling and aggregation at sensor nodes, while considering the maximum allowable delay for each message. By adeptly controlling the reception and aggregation processes of messages, the objective is to diminish energy consumption and optimize network performance.

The remainder of the paper is structured as follows: Section 2 reviews prior works, Section 3 delineates the proposed model along with the algorithms, Section 4 elaborates on the evaluation of the proposed approach, and finally, Section 5 outlines future prospects and draws conclusions.

2. Related works

The Internet of Things (IoT) encompasses a network that facilitates connecting uniquely identifiable objects to the internet. These objects possess the ability to sense stimuli and potentially execute programmed actions. By leveraging distinct identification and measurement capabilities, it becomes possible to remotely gather information or modify the status of these objects at any given moment, facilitated by any entity [26]. The Border Gateway Protocol (BGP) serves as a simplified alternative to MQTT for enabling connectivity between resource-constrained objects and the World Wide Web [27,28]. As BGP is a streamlined version of MQTT, establishing connectivity between web applications and the network is feasible using a transitive proxy, requiring minor modifications to request and response formats. Please establish the connection of the sensor.

BGP is designed based on the principles of the Representational State Transfer (REST) architectural style. Within this framework, a resource is a conceptual entity governed by the server, specifically the BGP server, which is designed to be installed on the sensor device [29]. Adhering to the BGP protocol enables access to the sensor's functionality. When designing the communication protocol for the application layer, it is crucial to consider constraints imposed by the sensor network, such as limitations on packet size and bandwidth. BGP is commonly used in Low-Rate Wireless Personal Area Networks (LR-WPANs), where IEEE 802.15.4 protocol limits packet size to 127 bytes per transmission [30]. Efficiency of the network may be compromised if increased packet transmission within the MAC layer occurs.

A Low-Rate Wireless Area Network (LR-WAN) is an affordable network facilitating wireless communication with minimal power usage and moderate data transfer rates. Its objectives include efficient data transfer, cost-effectiveness, and the use of a straightforward protocol [31]. Research [32,33] employs BGP routing protocol to achieve ideal Quality of Service (QoS) values across varying bandwidths, indicating improved performance compared to VoIP networks based on ITU-T G.114 standard. However, BGP poses

Table 1
Summary and comparison of existing approaches.

Ref.	Approach Name	Advantages	Disadvantages
[38]	LoW-PAN	- Facilitates IPv6 utilization in wireless networks with little data loss	May not efficiently handle constraints like limited RAM and processing capabilities
[39]	MQTT	- Dependable TCP connections - Suitable for secure communication	-Not specifically engineered for devices with limited RAM and processing capabilities
[40]	BGP	- Streamlined alternative to MQTT - Enables connectivity between IoT devices and web	Introduction of overhead and energy consumption
[41]	SDN	- Potential to mitigate BGP-related challenges -Cost-effective network administration	Challenges in scalability and privacy
[42]	Leh router	- Management of 16-bit short addresses in LoWPAN-based networks	Limited text provided for detailed advantages and disadvantages
[43]	IEEE 802.15.4	-Standard for LR-WPAN networks - Defines packet size limit of 127 bytes	Potential efficiency issues if packet transmission increases within MAC layer due to packet size limit
[44]	REST Architecture	- Facilitates access to sensor functionality through BGP server	Constraints of sensor network such as packet size and bandwidth must be considered
[45]	CSAM	- Minimizes overhead in small to medium data packets - Reduces energy consumption and network traffic	Requires implementation of scheduling and aggregation techniques at sensor nodes

security vulnerabilities due to authentication and validation challenges. Recent research suggests using Software-Defined Networking (SDN) to mitigate these challenges, but operational challenges remain [34].

Researchers aim to address challenges faced by BGP implementation of SDN, focusing on enhancing convergence speed while overlooking scalability and privacy concerns [34]. Address and destination field allocation within packets account for approximately one-eighth of available capacity within the Mecca layer [35]. LoWPAN-based networks assign management of 16-bit short addresses to the Leh router, facilitating neighbor discovery [36]. Wi-Fi enables HTTP-based web pages in proposed systems to send data to distant places, facilitating monitoring of weather changes [37]. The suggested weather station is advanced, precise, economical, and dependable, suitable for anyone wishing to track environmental changes regularly [37]. Table 1 compares different approaches in addressing IoT connectivity and communication challenges in wireless sensor networks, providing insights into their suitability for various scenarios.

3. Suggested method

This section presents the details of a proposed technique known as CSAM. The objective of this approach is to minimize the additional burden placed on small and medium-sized data packets within multi-hop networks that employ the BGP (see Fig. 2). Under normal conditions, BGP is not utilized in the suggested manner.

The nodes involved in packet forwarding can be in any of the following states: idle, where the individual anticipates an event's occurrence in the context of received processing and subsequent conveyance of said event. Henceforth, the term "sending" replaces the forward method. The rationale behind the node's status change is as follows: changing the status to 1 indicates readiness to accept packets; the processing event generates packets for sending. A status change to 2 occurs upon packet reception by the MAC layer. Transition to state 3 happens when $D(p)\neq n_i$, assuming that node n_i in Fig. 2's status diagram corresponds to it and that the technique *(Dst(p))* identifies packet *P's* destination. The process of receiving and sending the packet is depicted in the above diagram.

In BGP, the node's role is theoretically straightforward: packets are transmitted upon receipt. However, in practice, this may vary due to differing priorities among packets sent to different destinations [46–48]. IEEE 802.15.4 allows more efficient bandwidth use by aggregating packets or eliminating a portion of the aggregated packets' overhead during transmission. Consequently, transmission can reduce node energy consumption and extend the network's lifespan.

The network has successfully executed the tasks outlined in the present paper.

a) Organizing BGP requests and responses based on the network's transmission priority, while establishing the maximum allowable duration. Enclosed is a concise elucidation of the fundamental principles and practical implementation of the parameters, variables, and methodologies employed within the proposed methodology.
b) Managing message timing and aggregation on sensor nodes by controlling the reception process according to the maximum permissible delay for each message. Aggregated messages are subsequently placed in the designated destination. When the term "packet" is utilized without specifying its layer, it pertains to packages of the LoW-PAN network layer. Additionally, when packet or suitable size is used for aggregation, it indicates compliance with the requirement stated in (1) [49,50].

$$L(p) \leq CUR\_MAX\_PLD\_SZ\text{-}L(QB) \tag{1}$$

While the information transmitted in RFC 7641 may have varying priorities, it is transmitted with the same priority in networks built on BGP. For example, data regarding greenhouse humidity and gas leaks in smart buildings are transmitted via the network with equal priority [51,52]. The priority of BGP Control Management Protocol (CMP) messages is categorized into four levels, as specified in Ref. [8]. According to equation (2), this categorization serves the purpose of minimizing the impact of low-priority messages and leveraging them for network traffic management and optimization.

$$0 \leq CMP\ (p) \leq 3 \tag{2}$$

Three is the lowest priority level, whereas zero denotes the highest. BGP messages also need to include the value's storage location. The request identifier, also known as a token included in the structure of the BGP protocol, is employed by the client to determine the answer to its queries [53]. The priority of the CMP (BGP) message under consideration is inserted using the token's initial two bits in

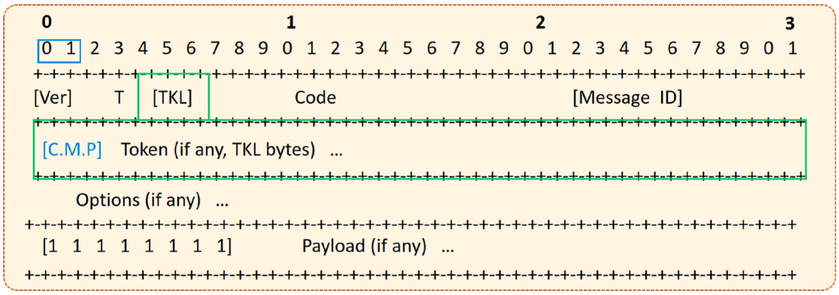


Fig. 2. Scheduling of critical information in a BGP message.

the network. CMP, situated where CMP is, Fig. 2, can handle both the issue of packet priority in the network and the issue of the customer's preferred priority while receiving the response. The client (in this case, the router) enters the field token in the request. The client submits the request to the BGP server by entering the necessary priority in the CMP. A smaller value indicates a greater priority when the server compares the priority of the requested subject with that of its source, incorporating the message. The client can use this method to set the packet priority for the network, provided that the requested priority does not drop below the server-specified priority. This feature has the advantage of allowing the proxy connected to web users to request a topic with greater importance depending on the requested queue [54,55]. As a consequence, the proxy can handle requests based on priority, which will improve the quality of its service. The Maximum Interval of Time that the network is permitted to deliver a packet from the MIDA to the destination is known as the maximum allowable delay, or MAD. Since each message priority (CMP) has a predetermined value, the suggested approach will begin as soon as the packet is received from the value. The value of the packet's maximum permitted delay can be extracted using two CMP bytes [56–58]. The maximum network timeout settings that are part of the BGP-based communication setup parameters must not conflict with MAD when it is chosen. The objective of calculating the total input and output of HASCO nodes (per equation (3)) during the BGP multi-step network's active period based on scent is

$$\text{minimize} \sum_{n_{i \in N \setminus ER}} \cdot \left|P^{I}_{n\ i} \right| + \sum_{n_{i \in N \setminus ER}} |P^{O}_{n\ \ i} \tag{3}$$

The performance of the suggested approach can be compared to the present performance of the BGP protocol stack using the objective function stated in (3). The effect of the proposed technique can be quantitatively verified by computing the above equation for both the suggested method and the S·P.S. method, assuming that the conditions and the value of $\sum_{n_{i\in N}} \mathrm{L}\ (P^{s}_{n\ \ i})$ are constant [59].

The CSAM approach influences the decrease in packets entered into the nodes upon receiving information from the router's edge, resulting in a reduced amount, including$| \sum_{n_{i\in N\setminus ER}} |P^{I}_{n\ \ i}$. Additionally, an effort is made to minimize the quantity of packets sent out from the nodes in order to send the answer from the sensor grams to the router, which produces a smaller result. With $| \sum_{n_{i\in N\setminus ER}} || P^{O}_{n\ \ i}$ The greatest amount of time that can be spent keeping the packet P on node n_i is specified as the cardinality sign in the preceding expression, which gives the quantity of the set's members $W^{P}_{n\ \ i}$. The longest period of time that can pass from the time a packet (p) is received until it is sent to node $| n_i$ is allowed [60,61]. This value, which stands for time, will be positive in accordance with equation (4).

$$W^{P}_{n\ \ i} \leq 0 \tag{4}$$

This value is equivalent, if the message is of type "C·O·N, N·O·N, or A.C·K″, to the lowest value between the maximum allowable delay and the maximum validity time of the data in the BGP packet, less the total time it takes for the packet to travel from the node to the destination (here, the router) [62,63]. The average amount of time required for package processing is found using (5).

$$W^{p}_{n\ \ i} < \min\{MaxAge(p), MAD(p)\} -) \tag{5}$$

$$\text{OW}\ D^{n_i}_{ER} - PT^{p}_{n\ \ i}$$

$$\forall_p \in P^{I}_{n\ \ i}, \forall_p \in P^{S}_{n\ \ i} : type(p) \in \{CON, NON, ACK\}$$

The maximum duration the node is allowed to keep the message is (6) is zero if the message is of the RST type.

$$W^{p}_{n\ \ i} = 0\ \forall_p \in P^{I}_{n\ \ i}, \forall_p \in P^{S}_{n\ \ i} : \text{type(p)} = \text{RST} \tag{6}$$

The network layer's size (LoW-PAN) packets that contain BGP messages is in the interval established in (7) according to the limits of the size of packets in networks based on 802.15.4 IEEE in the layer (MAC), as well as this layer's little packet overhead [64].

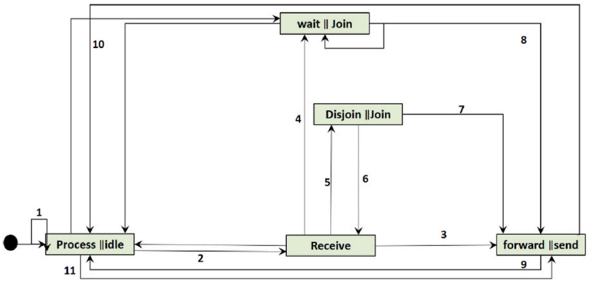


Fig. 3. Node status diagram in the suggested protocol for the LoWPAN BGP network node to receive and send packets.

$$\begin{aligned} &\text{MIN\_MAC\_OH} \; < \; \text{L(P)} \leq 127 \\ &\forall_P \in P^O_{n\ \ i}, \forall_P \in P^i_{n\ \ i}\, \forall_P, \in P^s_{n\ \ i} \end{aligned} \tag{7}$$

All phases of design will take the aforementioned constraints into account; for instance, in what follows, the value of $W^p_{n\ \ i})$ will be explained in terms of the BGP message type and its relative importance. The node status diagram from the suggested technique is shown below, along with the pseudo-codes that correspond to it [65,66,67]. The suggested method for the sensor node in the LoW-PAN/BGP network to receive and send packets is depicted in the status diagram shown in Fig. 3. An acceptable latency can be achieved in the aggregation and separation of packages by using the following techniques to manage the waiting states for connection and separation.

The status graph's numbers provide the following explanations for a node's change in state: If the node's state is 1, it is not actively listening for packets or preparing packet processing events for transmission. If the MAC layer receives a 2, it signifies the packet was successfully sent. If the third criterion in (8) holds true that is, whether the node receiving the packet makes a choice based on whether the packet is highly prioritized with the size information then the node will transition to the third state. It has not given enough time for the existing package to be satisfactory [68]. Therefore, packet will be sent to the next node, with almost no expectation on that node.

$$bs^p_{n\ \ i} = 1\ Dst \times (p) \neq n_j \big(CMP(P) = 0 \vee D.M.W\_Can\_Wait \big(CU - Max - P.L.D - S.Z - L.(p) - L.(Q \times B) - \Delta, W^p_{n\ \ i} \big) = 1 \big) \tag{8}$$

Fig. 4 shows the reduction of the additional load imposed on small and medium size packets based on the proposed approach.

The block diagram of Fig. 4 shows the key components of the proposed method and their mutual relationships in addressing the issue of reducing the load of small and medium packets in a network environment. Each of its components is briefly explained below.

Packet Classification: The process begins with classifying incoming packets into small, medium, and large categories based on their size.

Prioritization: Small and medium-sized packets are identified for prioritization due to their higher burden on the network.

Queue Management: A specialized queue management system is implemented to handle small and medium-sized packets separately from large packets.

Traffic Shaping: Traffic shaping techniques are applied to regulate the flow of small and medium-sized packets, ensuring smoother transmission and reducing congestion.

Buffer Allocation: Adequate buffer space is allocated for small and medium-sized packets to prevent packet loss and ensure efficient delivery.

Dynamic Routing: Dynamic routing algorithms are employed to optimize the path for small and medium-sized packets, minimizing delays and improving overall network performance.

Feedback Mechanism: A feedback mechanism continuously monitors network conditions and adjusts packet handling parameters accordingly to maintain optimal performance.

Quality of Service (QoS): Quality of Service mechanisms is utilized to prioritize small and medium-sized packets over less critical traffic, ensuring timely delivery of important data.

End-to-End Encryption: To enhance security, end-to-end encryption is employed to protect the confidentiality and integrity of small and medium-sized packet payloads.

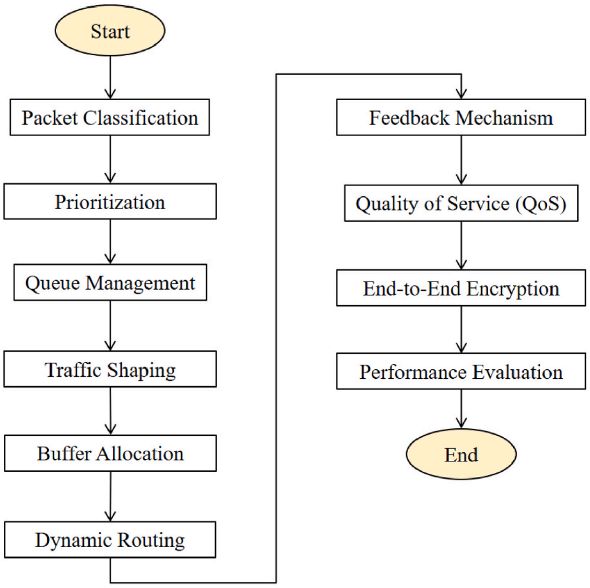


Fig. 4. Flowchart of the overhead reduction process imposed on small and medium size packets.

Performance Evaluation: The performance of the proposed method is evaluated through simulations or real-world testing to assess its effectiveness in reducing the burden on small and medium-sized packets while maintaining network efficiency and reliability.

If a BGP message is contained in the received packet, its destination is not the current node, and its priority is low or the decision component to wait for the received packet, then the state transition to (9) is triggered or has estimated the package's suitable dimensions and delivery time [69].

$$\begin{gathered} bs^{p}_{n\ \ i} = 1^{\mathrm{Dst}} \times (\mathrm{p}) \neq n_j\big(CMP(P) = 1 \\ D.M.W - Can\_Wait\big(CU\_Max - PLD - SZ - L(p) - L \times (Q.B) - \Delta, W^{p}_{n\ \ i}\big) = 0\big) \end{gathered} \tag{9}$$

While waiting, the following tasks are carried out: The value w is utilized if the W.T timer does not already have a value; if not, the lowest value between the current W.T and is used [70]. (a) Setting the W.T timer in accordance with (10). In other words, the maximum delay permitted the packet to is used to adjust the W.T timer value at the moment of reception so that It is possible to add the packet to the Q. B waiting list.

$$\mathrm{W.T} \leftarrow \min\{\mathrm{W.T}, W^{p}_{n\ \ i}\} \tag{10}$$

b) Inserting the package in the QB queue finder

Q. B←Join (p,Q.B)

c) awaiting the next packet to arrive until the circumstance in (11) is satisfied. In the event where just (Q.B)L is greater than zero, the WT or Q. B timer will be reset, Q. B will be sent, and the value of CMP (P) will be updated [71].

$$0 \leq L(QB) < CUR\_MAX\_PLD\_SZ - \lceil^{W} T \neq 0^{D} MW\_CanWait(CUR\_MAX\_PLD\_SZ - L(QB) - \Delta, WT) = 1 \tag{11}$$

If the specified condition holds true, i.e., there are multiple messages in the packet that was received, then the status 5 transition will take place [70]. This means that the received message is a collection of sub-packets, each of which is a message for the UDP/BGP layer. equation (12) shows these conditions.

$$If\ bs^{p}_{n\ \ i} = 1\ then\ \forall\ sub^{p}_{j} \in S\ if\ Dst\big(sub^{p}_{j}\big) = n_i, Dis\_join\big(sub^{p}_{j}, S\big) \tag{12}$$

In the event where the current node is the extracted packets' destination, then the usual receipt of the package will be emulated by the receipt of status change No. 6 following each separation or preparation of the buffer and method call. equation (13) shows these conditions.

$$If\ bs^{p}_{n\ \ i} = 1\ then\ \forall\ sub^{p}_{j} \in S\ if\ Dst\big(sub^{p}_{j}\big) = n_i, Dis\_join\big(sub^{p}_{j}, S\big)\ and\ call\ Receive\big(p_j\big) \tag{13}$$

Using equation (14), in updating the number's status, per the stipulation in After each partition, packets are aggregated according to path sharing, and then the forward procedure's sending method is invoked should the extracted packets' destination not be the current node.

$$If\ bs^{p}_{n\ \ i} = 1\ then\ \forall\ sub^{p}_{j} \in S\ if\ Dst \times \big(sub^{p}_{j}\big) = n_k : n_k \neq n_i\ Disjoin\big(sub^{p}_{j}, S\big)\ and\ Join\big(sub^{p}_{j}, P_K\big).\ Call\ Forward(P_k) \tag{14}$$

Change of status number 8 transpires when the package becomes amenable to amalgamation with number 28, while the status change of number 9 transpires upon invocation of the packet sending method within the LoWPAN layer. In the context of the message exchange mechanism, a distinct algorithm exists for the process of retrying [72]. Consequently, the failure to transmit, as depicted in Fig. 5's status diagram, is of negligible significance. This failure is specifically associated with the LoWPAN layer within the

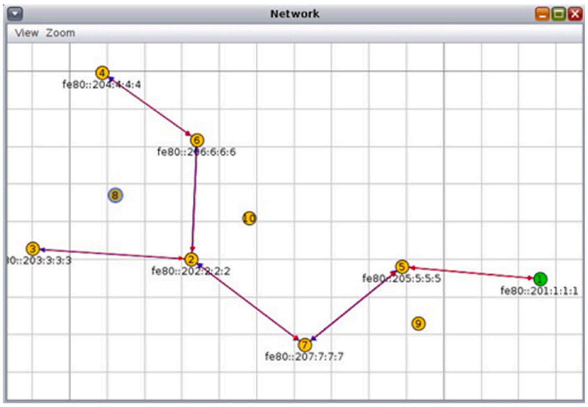


Fig. 5. Information transfer that has been aggregated in multiple steps.

LoWPAN/BGP protocol stack. It is assumed that the packet generated by the node for this purpose is not a crucial concern. The occurrence of circumstance number 10 is contingent upon the fulfillment of the aforementioned criterion, as it serves as the means by which an event in the environment is seen (equation (15)).

$$\begin{gathered} CMP\left(P_g\right) \neq 1 \\ \left(D.M.W - CanWait\left(CU - Max - P.L.D_{L\left(P_g\right)} - L \times (Q.B) - \Delta, W^{p}_{n\ \ i}\right) = 0\right) \end{gathered} \tag{15}$$

The change of status number 11 occurs when the conditions mentioned in equation (16) are met.

$$CMP\left(P_g\right) \neq 1 \vee \left(D.M.W - CanWait\left(CU - Max - P.L.D_{L\left(P_g\right)} - L \times (Q.B) - \Delta, W^{p}_{n\ \ i}\right) = 1\right) \tag{16}$$

The suggested status diagram provides explanations for the key pseudo-codes of waiting and separation statuses, which are described in mathematical form in the following pseudo-codes. Algorithm 1 outlines the process of transitioning between states 6 and 7.

Algorithm 1: Obtain a pseudo-status code.

```
Algor. Acquire
    Packet Received s
    Void output (Note: The procedure Acquire (p), which processes the gotten the packet in a node) $bs^{s}_{n\ \ i} = 1$) and Dst × (s)$\neq n_j$ then if
    If C.M.P × (s) = 1 then
      Go ahead(s) else if C.M.P × (s)≠1 and D.M.W-CanWait × (CU-Max-s.L.D-SZ_L × (s)-L × (QB)-Δ, $W^{p}_{n\ \ i}$) = then
        invoke Wait(s)
          end if
    end if
    if ($bs^{s}_{n\ \ i} = 0$)
          Dis_join ($sub^{p}_{j}$,S)
    Reenter
```

Algorithm 2: pseudo-code and the state of separation

```
Algor. Dis_join
    Packet Received s
    Void output
    Note: Dis_join(s) technique, Pull subpackets out of the input and calculate the next state if ($bs^{p}_{n\ \ i} = 0$) then
      for each $sub^{p}_{j}$ in S do
    $p_j$ ←Extract ($sub^{p}_{j}$,S)
        If Dst ($s_j$) = $n_k$ and $n_k \neq n_i$ then
    Next hop grouping and joining ($s_j$, $s_k$) else if Dst × ($s_j$) = $n_i$ then
          call Receve ($s_j$)
          state←Receve
            end if
    end loop
    call Forward ($s_k$)
            state←Forward
    end if
    return
```

Algorithm 3: status of waiting for pseudocode

```
Algor. await
    Packet Received s
    Void output (Take note: keep packets in the queue buffer using the wait(s)method, take into account admissible packet delay and DMW_CanWaited Receive packet length)
    W.T←min{W.T, $W^{P}_{n\ \ i}$ }
    Q × B ← Join × (s,Q × B)
    While 0 ≤ L (QB) < Max-s.L.D_SZ (SUR- MAX PLD S.Z-L (Q × B)-Δ,W.T) = 1 do
      Await the incident
        When receive_event = event, then
          W.T←min{W.T, $W^{P}_{n\ \ i}$ }
            Q × B←Join × (p,Q × B)
        else if Time_event = event
               proceed
            end if
        end while
        W.T←0
```

(continued on next page)

(*continued*)

Algorithm 3: status of waiting for pseudocode

```
        Call Forward (Q × B) state←Forward
        Return
```

Algorithm 4: pseudo-code indicating the status of sending and forwarding

```
Algorithm Forward
    Packet Received s
    Void output
        Output ($p_{in}$ $p_{in}$ ←null
            state←Idle
                return
```

Algorithm 5: pseudo-code indicating overload or idleness

```
Process of Algorithm _Generated _ Packet
    Packet Received s
    Void output if C.M.P ($s_g$)≠1 and (D.M.W _CanWait ($s_g$) –L(Q × B) -Δ, $w^p_{n\ i}$ = 1) then
    call Wait ($p_g$)
    state ← wail
    else if CMP($p_g$) = 1 or (D.M.W _CanWait × L(Q × B) -Δ, $w^p_{n\ i}$) = 1)then
        call Forward ($p_g$)
            state←Send
                return
```

Based on the data provided in the 2011 standard, it is stated that the maximum packet size within the Low-Rate Wireless Personal Area Network (LANCAP) is denoted as MAX_PLD_SZ and is equivalent to 116 bytes. This is done to effectively utilize memory and minimize the computational load associated with processing received packets. The range of their length spans from 6 to 116 bytes [17, 73]. The act of categorization is undertaken. The default method of classification involves utilizing a 10-byte format, and the determination of a packet's length class is computed based on equation (17).

$$C_L\left(P^I_{n_i}\right) = \frac{L(P^I_{n_i})}{10} + 1 \tag{17}$$

Therefore, in the 6th LoWPAN layer, the class number of the length of the nodes will always be equation (18).

$$1 \leq C_L(P^I_{n_i}) \leq 11 \tag{18}$$

Based on the provided information, it is feasible to establish tables for categorizing BGP messages based on the priority and length class of each message. These tables, denoted as $T^1_{n\ i}$‘ $T^2_{n\ i}$ and $T^3_{n\ i}$ encompass a total of eleven dimensions, with 3 × 11 being specifically designated for this purpose. Henceforth, the term "message class" (namely, the class denoting the priority and duration of a message) has been ubiquitously employed within a tabular context. This refers to the precise location of a residence listed in the aforementioned tables. The residence can be identified by its row value, denoted as $C_L(P^I_{n_i}$, and its column value, denoted as CMP $\left(P^I_{n_i}\right)$, within the table. The score attribute within the structure of table $T^3_{n\ i}$ represents a numerical indicator of the system's performance, which is influenced by the time intervals of the inputs. An increment of one unit will be made to this value. Conversely, if the prediction of the maximum time for receiving the next packet is inaccurate due to the dynamics of the environment and the corresponding dynamics of the input time, a deduction of one unit will be made from this value. As a result, the numerical value allocated to the score field will be either negative or positive, depending on the performance of the system. In the event that the value is greater than or equal to zero, it is imperative for the system to transition into a state of waiting. The inclusion of a control field serves the objective of enabling the distinction between the observations and predictions made by the system, hence facilitating the subsequent process of decision-making. To provide more clarification, assuming that the initial value of this variable is negative and increases by one for each favorable outcome, the system commences action only after it has already attained a successful prediction.

Within the table's structure, the reset_counter field $T^3_{n\ i}$ is capable of assuming discontinuous values ranging from 0 to 3. Furthermore, in the event that the system score is equal to -, the reset_counter continues to be incremented. In the event that the value of reset_counter reaches a value of 3, the house that shares the same priority length class as indicated in table $T^2_{n\ i}$ will undergo a reset, resulting in the restoration of its standard amount. The purpose of this reset is to mitigate the risk of the algorithm becoming trapped in a state of maximum value as a result of significant fluctuations in the time intervals for receiving messages of a specific class (referred to as priority length). This is due to the fact that each house $T^2_{n\ i}$ consistently experiences the maximum number of time intervals for receiving messages of that particular class. The prognosis has been revised to offer a more plausible forecast based on the most adverse encounter. Consequently, by resetting this number, it serves to mitigate the algorithm's susceptibility to temporal variations. The structure of the table contains a reserved field denoted as table $T^3_{n\ i}$. A binary value is present within the control structure of the table.

In the event that the value of this particular field is equivalent to 1, it signifies that a message has been inserted into the waiting queue for subsequent merging with the current message. Consequently, until the message exits the waiting queue, the associated message class will not be regarded as a priority for merging with other messages. The elucidation of the decision system algorithm will provide a more comprehensive understanding of the role of this aspect in the determination to delay. The statistical variables are the measurable characteristics or attributes that are being studied or analyzed in a statistical analysis. The effectiveness of TP (True Positive) and FP (False Positive) measures is closely associated with the performance of the Dynamic Model of Warfare (DMW) inside a dynamic environment. The IP variable represents true positive occurrences, which arise when the DMW successfully receives a packet within a designated time period. Conversely, the FP variable denotes false positive instances, which occur when the DMW incorrectly estimates packet reception within a specific time frame, despite the packet not actually being received during that period. The positive predictive value (PPV) quantifies the probability of the DMW forecast accurately manifesting. The calculation of the positive predictive value (PPV) is derived from equation (19).

$$\mathrm{PPV} = \frac{TP}{TP + FP} \tag{19}$$

During the course of DMW's operation, the true positive (TP) and false positive (FP) values are continuously updated in real-time. Whenever deemed essential, DMW utilizes these updated values to inform its decision-making process. Specifically, DMW employs a calculation to determine the positive predictive value (PPV), comparing it to the previously calculated PPV value. If the current PPV value surpasses the previous value, DMW prioritizes this updated PPV value in its decision-making. When the Positive Predictive Value (PPV) exceeds or is equal to the minimal prediction value that the system needs operation (MIN_PPV), the system executes actions according to DMW choices. Otherwise, the system just makes observations and does not transition to The state of waiting. The entire performance of D.M.W is regulated through the use of PPV. The Min P·P·V value is specified as a parameter in the D.M.W setup, with a range of values from 0 to 1. The Decision Component (D.M.W) algorithm for waiting consists of the following steps.

Algorithm 6: Initialization pseudo code for DMW components

```
Algorithm D.M.W Initialize input _void
    output _void
    $T^3_{n\ i}$ do $T^2_{n\ i}$, for each $T_{ni}$ [i] [j] in $T^1_{n\ i}$ ,
    $T^1_{n\ i}$ [j][i] ← −1
    $T^2_{n\ i}$ [j][i] ← −1
    $T^3_{n\ i}$ [j][i] score ← −1
    $T^3_{n\ i}$ [j][i] reserved ← 0
    $T^3_{n\ i}$ [j][i] reset counter ← 0 end loop
    T.P← 0
    F·P← 0 return
```

The tables $T^1_{n\ i}$, $T^2_{n\ i}$ and $T^2_{n\ i}$ are initialized with values that are both illegal and default. The priority length of a message class is determined. Table $T^1_{n\ i}$ is modified according to the timestamp at which the packet is received in the respective class. The square of the sum of n and i yields a larger value, which is then assigned to the appropriate location within the table representing the relevant dwelling. In the event that the value of the associated element in table $T^2_{n\ i}$ is substituted having a value greater than the field for scores value of the corresponding house in table $T^3_{n\ i}$, a deduction of one unit will occur. If the value of this field persists as −1 for a maximum of three consecutive failures, the corresponding in the tables' values $T^2_{n\ i}$ and $T^3_{n\ i}$ is going to reset. This step prevents the algorithm from being affected by the greatest values of the distance between two arrivals resulting from temporal variations. In addition, the value of false positives (FP) increases by one unit for each instance of failure. One unit is added to the value and score field from the relevant house in the table $T^3_{n\ i}$. Moreover, zero (5) is entered in the reset_counter columns. At this juncture, the algorithm makes a determination according to three criteria to ascertain if the package is capable of being held for aggregation with the corresponding package in relation to its size.

In the event that the system has achieved a favorable outcome in its predictive capabilities, it is necessary for the score value to be equal to or greater than zero. Additionally, the current class must not have been saved for the package awaiting another one, indicated by a reserve value of zero. The initial step of the aforementioned technique entails the initiation process of time tables and the control table. Steps two to four are relevant to the updating process.

Algorithm 7: The observer section of the pseudo code of the D.M.W component on the incoming traffic of the node

```
Algorithm DMW_GetPackets_Received_Info
    Input $P^I_{n\ i}$ output void (note: $DM_{GetReceivedPackets\_}$ Info ($P^I_{n\ i}$) method)
    $I = C_l\left(P^I_{n_i}\right)$
    J = CMP($P^I_{n_i}$)
    If ($T^1_{n\ i}$ [j][i]≥0)then
        TimeDiffBetween2Receive = ReceivedTime $\left(P^I_{n_i}\right)$- $T^1_{n\ i}$ [j][i] end if
```

(continued on next page)

(*continued*)

Algorithm 7: The observer section of the pseudo code of the D.M.W component on the incoming traffic of the node

```
    $T^1_{n\ i}$ [j][i]← Received_Time $\left(P^I_{n_i}\right)$
    If ($T^2_{n\ i}$ [j][i] $\geq$ 1) then
    If Time_Diff_Between_2_Receive > $T^2_{n\ i}$[j][i] $\geq$ 0then
    $T^2_{n\ i}$ [i][j]← Time_Diff_Between_2_Receive if ($T^3_{n\ i}$ [j][i] reset counter $\geq$ 2) then
    $T^2_{n\ i}$ [j][i] ← −1
     $T^3_{n\ i}$ [j][i] score ← −1
    $T^3_{n\ i}$ [j][i] reserved ← 1
    $T^3_{n\ i}$ [j][i] reset counter ← 0 end if
    if ($T^3_{n\ i}$ [j][i] score = −1) then
     $T^3_{n\ i}$ [j][i] reset counter –else
     $T^3_{n\ i}$ [j][i] score ++ end if
    F·P ++ if ($T^3_{n\ i}$ [j][i] score < 0)then
    $T^3_{n\ i}$ [j][i] score++ end if
     $T^3_{n\ i}$ [j][i] reset counter ← 0
    If
     $T^3_{n\ i}$ [j][i] reserved ← 0 else
     $T^2_{n\ i}$ [j][i] ←0 end if
    ruturn
```

The time tables and system control table play a crucial role in the decision-making process, particularly at step 5. The components of the DMW are depicted in the form of pseudo-codes below, used at different phases of the system state diagram. Algorithm 6 introduces the process of initializing the DMW component, while Algorithm 7 outlines the monitoring aspect of the DMW component as it pertains to the incoming traffic of the received packet flow node within the LoW-PAN layer.

The decision regarding whether to maintain a packet on the node includes a pseudo component.

Algorithm 8: pseudocode of the DMW component's decision-making section.

```
Algorithm D.M.W Can_Wait input L, $W^P_{n\ i}$
    output 1 or 0
    for j = 0 to $C_l$ (L) do
      for i = 0 to get CMP ($W^P_{n\ i}$) do
        if $T^1_{n\ i}$ [j][i] >0 then
          if $T^2_{n\ i}$ [j][i]$\leq$ $W^P_{n\ i}$ and $T^3_{n\ i}$ [i][j].reserved = 0 and $T^3_{n\ i}$ [i][j].score$\geq$ 0 then
          $T^3_{n\ i}$ [j][i] reserved ←0
          If TP = 1 return 1
          PPV←($\frac{TP}{TP+FP}$)
    If (P·P·V $\geq$ pastP.P·V) or (P·P·V $\geq$ Min_P·P·V) then pastP.P·V←P·P·V
            return 1
          else
            pastPPV←PPV
    return.
    end if
    end if
    end if
          end loop
          end loop
          return.
```

The presentation of the "waiting direction" is depicted in Algorithm 8. The variable "pastPPV" in this pseudo code is a local and static floating-point value with a starting value of zero. This section introduces the suggested methodology outlined in the paper, which aims to minimize the physical layer overhead and IEEE_802.15.4 MAC on Low-Power Wide-Area Network Packets. The objective is to enable the transmission of concise messages using the BGP protocol, specifically for applications such as monitoring. The solution being suggested exhibits a low computational burden and is suitable for implementation on nodes that possess constrained resources. Furthermore, the LoW-PAN protocol stack operates independently of the conventional layers, namely the MAC and physical network layers. This characteristic ensures that its functionality remains concealed from the user's perspective. In the subsequent section, we will assess the favorable impact of the suggested methodology on the round's energy usage and network impact, in comparison to the fundamental architecture of the BGP protocol stack. This evaluation will be conducted within the context of multi-hop networks, where monitoring is employed and the objective is to facilitate tiny data transmission.

4. Discussion and evaluation

In this section, the performance of the recommended approach is examined and analyzed after the introduction of quantitative indicators for assessing its performance. The recommended method's performance is assessed by contrasting it with the standard protocol stack's performance, which is described in Ref. [29] and will be referred to as "S·P·S." from now on. The programming language used to program the pseudocodes is C++ and more recently, the cooja simulator [9] in the contiki operating system [10,33] has been used to reduce the stack overhead of the IEEE 802.11.4 AN protocol for sending application layer data. Contiki incorporates a low-power processing engine known as Erbium, which effectively implements the BGP [33]. Additionally, Contiki utilizes Copper, a browser extension for Firefox, to facilitate BGP/Observe queries over the internet to a comparable network. The utilization of Cooja in the development process has been taken into account due to the primary focus of the proposed methodology being the reduction of traffic originating the edge router from sensor nodes. This approach is particularly relevant in applications involving the evaluation of performance indicators related to packet transmission from sensor network nodes to the edge router in multi-step networks based on 6LoWAN/BGP. The subsequent sections introduce monitoring applications within this context.

4.1. *Percentage of success in reducing outgoing packets (**SP_t^N**)*

Given the scenario where packets are being transmitted from within the link to the peripheral router, the use of the SPN index serves as a metric to quantify the decrease in the overall quantity of packets transmitted between the edge router and the sensor nodes, in relation to the total number of outgoing packets in the S·P·S technique, up until a specific time denoted as t. The value of the variable is determined by the calculation outlined in equation (20).

$$SP_t^N = \frac{M_t^N}{X_t^N} \times 100 \ \mathrm{Dst(p)} = \mathrm{ER}, \forall p \in P^I_{n\ i}, \forall p \in P^s_{n\ i} \tag{20}$$

The variable M_t^N represents the qantity of decreased packets originating based on sensor nodes' output, excluding the router (edge), as a result of implementing the suggested approach. This reduction is observed from the commencement of network operation until time 4. The value of M_t^N is computed using equation (21). The symbol X_t^N represents the numerical value as well. The cumulative count of receiving or created packets in the S·P·S technique for all sensor rounds (except the edge router) from the network's initiation to the moment of its evaluation at time (22).

$$M_t^N = \sum_{n_i \in N \setminus ER} \left| P^I_{n\ i} \right| + \sum_{n_i \in N \setminus ER} \left| P^s_{n\ i} \right| - \sum_{n_i \in N \setminus ER} \left| P^o_{n\ i} \right| \tag{21}$$

$$X_t^N = \sum_{n_i \in N \setminus ER} \left| P^I_{n\ i} \right| + \sum_{n_i \in N \setminus ER} \left| P^s_{n\ i} \right| \tag{22}$$

4.2. *The amount of traffic reduction varies based on the protocol stack's performance and application*

Network traffic refers to the quantity of data being transmitted via a network at a specific moment, and is influenced by a range of structural and environmental factors and variables. Traffic congestion is primarily attributed to two factors: application usage and performance. The former refers to the response of users to observations made about them, such keeping an eye on applications, while the latter pertains to the efficiency and effectiveness of the system in handling the influx of users. The measurement of this traffic is influenced by two parameters: PHY_OH overhead, This concerns the physical layer, as well as the overhead of ACK_OH acknowledgment, also related to the physical layer. This information is presented in Table 2. The serial is consistently applied to the packet during the transmission of MAC layer packets.

In the event that the sender of the packet has designated the authentication request (AR) field inside the MAC packet header as 1, it is imperative for the recipient to transmit an authentication packet as a kind of reply. Table 3 presents the composition and additional costs associated with this packet, considering the network layer's reduction of every packet. The physical layer overhead (PHY_OH), the MAC layer's current overhead (CUR_MAC_OH), and the acknowledgment message's overhead (ACK_OH) all diminish as more data is gathered. Hence, the quantification of the reduction in static traffic, measured in bytes (RTR_t^N) during the specified time interval, may be derived from equation (23).

$$RTR_t^N = M_t^N \times (P.H.Y\ O.H + C.U.R\ M.A.C\ O.H + A.C.K_O.H) - \ M_t^N\ b_{yt}e \tag{23}$$

Table 2
IEEE802.15.4 version 2011's physical layer packet structure.

PPDU arrangement	
PSDU	Header of PPDU
Package for Mac Layer	Synchronization Header Packet (SHR) Length
inside 127_bytes	4 bytes to 1 byte to 1 byte

Table 3
The MAC layer authentication packet structure and size from the 2011 edition of IEEE802.15.4

	At the MAC layer, the acknowledgment packet header	
Check the frame **2 byte**	field for sequence numbers 1 byte	field for frame control 2 byte

The negative symbol employed in this correlation signifies that the act of decreasing each package from the overall output entails its amalgamation with another package. The overhead of aggregation is one byte, resulting in a decrease in the number of reduced packets compared to the total number of deleted packets. The value assigned to a node is determined by the reduction in output size, measured in bytes, and is calculated using equation (24).

$$\mathrm{RTR}_t^{n_i} = \mathrm{M}_t^{n_i} \times (\ \mathrm{P.H.Y\ O.H} + \mathrm{C.U.R\ M.A.C\ O.H} + \mathrm{A.C.K_O.H}) - \ \mathrm{M}_t^{n_i}\ \mathrm{b_{yt}e} \tag{24}$$

The variable $\mathrm{M}_t^{n_i}$ represents the quantity of packets that have been diminished from the output of node n_i. On the other hand, $\mathrm{RTR}_t^{n_i}$ is utilized to determine the decrease in energy consumption within the node. Furthermore, the proposed approach allows for the computation of the average reduction in dependent traffic using equation (25).

$$\mathrm{RTR}_1^N = \frac{RTR_t^N}{t}\ byte/s \tag{25}$$

4.3. *The amount of reduction in depending on the performance and application, energy usage of the ($RTR_{n_i}^{n_J}$) (LON-PAN) protocol stack*

In order to determine the energy consumption associated with the transmission of a single byte within a network, it is necessary to account for both the energy required for packet transmission and the energy required for packet reception. In the event of a single-step transfer, or under the assumption of uniform heat distribution within the network, the constancy of environmental conditions, two factors are taken into consideration: the linearity of the energy calculation algorithm and the fixed distance between the source and destination.

The amount of energy used in the network to send a single byte is determined by using the formula for packet consumption in Ref. [34] equation (26).

$$E^1 = E_{send}^1\ + E_{Receive}^1 \tag{26}$$

The energy necessary to transmit one byte from node i to a nearby node in a single step is denoted as E_{send}^1 , whereas the energy required for node j to receive the same byte is denoted as $E_{Receive}^1$. Based on the aforementioned information, the degree of decrease The calculation of the energy required for transmitting packets from node n_i to node n_j is determined by equation (27).

$$\mathrm{RTR}_{n_i}^{n_J} = \left(\ E^1 \times \mathrm{H}_{n_i}^{n_J} \times \mathrm{RTR}_t^{n_i}\right) - \left(\varepsilon \times \mathrm{M}_t^{n_i}\right) \tag{27}$$

The symbol $\mathrm{RTR}_\mathrm{t}^{\mathrm{n_i}}$ represents the reduction rate of the amount of bytes transmitted by the node till time t. $\mathrm{H}_{\mathrm{n_i}}^{\mathrm{n_J}}$ denotes the number of steps from $\mathrm{n_i}$ to $\mathrm{n_j}$, and 3 represents the average amount of computing power required at node $\mathrm{n_i}$ to aggregate the packet. By utilizing equation (27), it becomes feasible to compute the extent of energy consumption reduction within the entire network, taking into account the correlation between the weight of grams and the flow trajectory of packets originating from the network's nodes to the Leh router. This calculation considers the energy quantity of TmoteSky sensors as mentioned in Ref. [34]. The simulator employs TmoteSky and the energy consumption associated with the 2420 C C radio component for transmitting one byte, which is equivalent to the value specified in Ref. [33], denoted as mj with a value of 0.12. Hence, equation (27) can be reformulated as equation (28) specifically for the TmoteSky platform equipped with the 2420 C C radio component.

$$RTR_{n_i}^{n_J} \cong 0/24 \times \mathrm{H}_{n_i}^{n_J} \times \mathrm{RTR}_t^{n_i} \tag{28}$$

In reference [33], it has been established that the energy consumption required to transmit a single bit is equivalent to the energy

Table 4
The suggested method's network simulation parameters and values.

measure	amount
The dimensions of the application layer packets that are generated	17–25 bytes
Network layer packet size (LoWPAN6)	41–55 bytes
Package size in the Mac layer	67–79 bytes
The total amount of packets generated throughout the simulation on every node	215 packages
The duration of the node's packet creation	515–4584 years
simulation duration	600 s
Priority of packets (CMP)	3 (Notes with standard priority)
The Maximum Allowed Time (MAD)	6 s
PPPV MIN	0.96

expenditure for executing 700,000 calculations. Consequently, the computational overhead is disregarded in light of the efficiency of the algorithms employed in the suggested approach. Hence, equation (28) can be simplified. The quantification of energy conservation in the transmission of a single bit can be feasibly computed.

The second, third, fourth, and sixth grams encompass the recording of themes for further viewing. The events associated with these grams possess a byte value ranging from 5 to 13. Table 4 presents a compilation of the key attributes of the simulated network, together with the parameters associated with the suggested methodology.

In the depicted topology, as seen in Fig. 6, the transmission of information from node 2 to the edge router occurs within a span of 3 steps. Similarly, the aggregated packets originating from node 4 and A traverse a path of 4 steps to reach the edge router. This process aims to evaluate the effectiveness of lowering outgoing packets, hence determining the success rate in terms of percentage. The preparation process lasted for a duration of 10 min. Fig. 6 displays the outcomes obtained from executing the algorithms of the proposed technique on the packet forwarding data generated within the network, in comparison to the S·P·S method, while maintaining identical settings. The provided information presents the data diagram illustrating the packet transmission originating from node 2, featuring the configuration depicted in Fig. 7. The red graphic pertains to the standard functioning of the network, namely the quantity of packets transmitted by node (2) when forwarding the packets received from nodes 6 and 7. The numerical value exhibited is 3. The presented blue diagram illustrates the progressive reduction in the number of packets transmitted from node 2 over time, as a result of executing the DMW algorithms associated with the proposed technique on the data stream, while maintaining identical conditions. The suggested method calculates the SP_t^N index, which quantifies the percentage improvement in the total number of reduced packets throughout network operation. Naturally, the optimization process is influenced by the approximate sequencing of events that occur inside various dynamic settings (equation (29)).

$$SP^N_{t=600} = \frac{109 + 220 \times 3}{1897} \times 100 = \%40/6 \tag{29}$$

During 600 s, the total dependent traffic reduction for the simulated network utilizing the suggested strategy as per (24) is equal to equation (30):

$$RTR^N_{t=600} = M_t^N \times \left(PHY_{OH} + CUR_{MAC_{OH}} + ACK_{OH}\right) - M_t^N = (109 + 220 \times 3) \times (6 + 21 + 11) - (109 + 220 \times 3) = 28453\ Byte \tag{30}$$

Also, the average reduction of dependent traffic for the network simulated when using the suggested method in place of the S·P·S method is equivalent to equation (31).

$$RTR_1^N = \frac{RTR^N_{t=600}}{t} = \frac{28453}{600} = 47/42\ byte/s \tag{31}$$

The simulated network's Node 2 is found to be a bottleneck, thus reducing traffic on such nodes might provide favorable outcomes in terms of network efficiency and longevity. Fig. 8 illustrates the utilization of the suggested traffic methodology through the computation of the output traffic of node number 2. The observed outcome of this particular node has exhibited a decline.

Equation (32) demonstrates the linear correlation between traffic reduction and energy consumption. Consequently, Fig. 8 illustrates that the energy consumption of node 2 reduces during the simulation period.

$$RES \cong RES^{n_2}_{n_6} + RES^{n_1}_{n_2} = \left({}^{0}\!/\!{}_{24} \times 1 \times 109 \times 38\right) + \left({}^{0}\!/\!{}_{24} \times 3 \times 220 \times 38\right) = 7013\,/\,28\ mj \tag{32}$$

Fig. 8 depicts the aggregate count of packets generated within nodes and the cumulative count of packets exchanged between nodes during the course of the 600-s simulation. Based on the aforementioned findings, the conducted experiments indicate that the

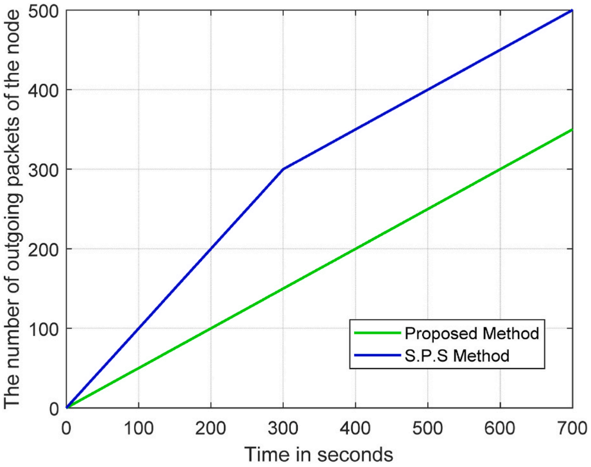


Fig. 6. The quantity of output packets coming from the second node (in 600 s) that separates the S·P·S method from the suggested approach.

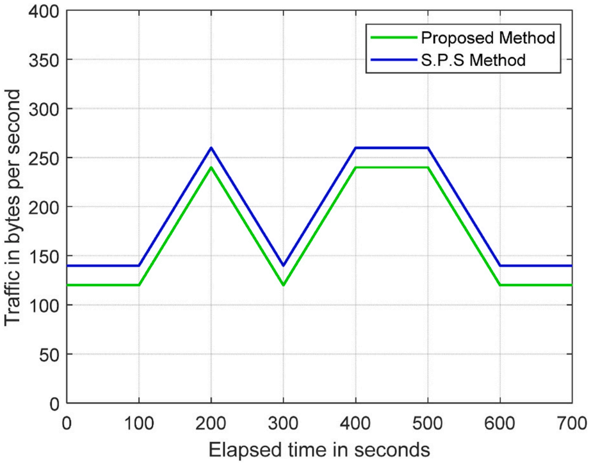


Fig. 7. The variance, measured in 600 s, between the S·P·S approach and the proposed method for the outgoing traffic of node number 2.

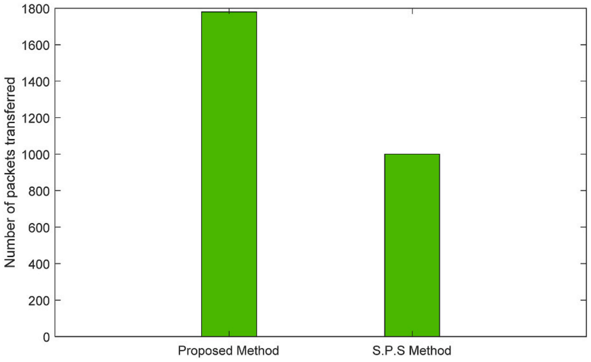


Fig. 8. Comparison of the S·P·S technique and the proposed method's total network traffic (measured in packets per 600 s).

utilization of the suggested approach in multi-channel networks is advantageous for applications involving the monitoring of periodic alterations in subjects with compact packages, necessitating regular notifications to the central system. The implementation of a step utilizing the BGP protocol stack results in a decrease in both network traffic and energy usage.

The findings of the conducted research significantly reinforce the results of previous research while also introducing new innovations not found in earlier studies. Firstly, the research builds upon previous work by addressing the challenge of reducing overhead and energy consumption in multi-temporal networks using the Border Gateway Protocol (BGP). Previous studies, such as [29], have highlighted the overhead introduced by the BGP protocol stack and its impact on network performance. By proposing the Critical Information Scheduling and Aggregation Method (CSAM), the current research offers a novel approach to mitigate this overhead. This method involves scheduling and aggregating BGP packets at sensor nodes, prioritizing packet transmission, and managing message scheduling to optimize network performance. These strategies align with the goals of previous research, which focused on improving efficiency in IoT networks. Additionally, the evaluation of the proposed approach provides empirical evidence supporting its effectiveness in reducing network traffic and energy consumption. For instance, the analysis of experimental results demonstrates a decrease in CPU utilization, path convergence time, and traffic consumption compared to standard methods like the S·P.S. technique. These findings reinforce the conclusions drawn from previous research, such as [33], which also emphasized the importance of optimizing network resources for improved performance. By quantifying the reduction in outgoing packets, traffic consumption, and energy usage, the current study provides concrete evidence of the benefits of implementing CSAM in IoT networks, corroborating the theoretical findings of earlier research.

However, the conducted research also introduces new innovations not found in previous studies. For example, the proposed method incorporates techniques for categorizing BGP requests and responses based on priority, as well as managing message scheduling considering maximum allowed delay. These aspects were not extensively explored in previous research and represent novel contributions to the field. Furthermore, the study evaluates the performance of CSAM using a simulation environment with specific parameters and metrics, providing detailed insights into its effectiveness under different scenarios. This level of experimentation and analysis goes beyond the scope of previous research and contributes to a deeper understanding of the practical implications of optimizing BGP in IoT networks. Overall, while the findings of the conducted research reinforce the results of previous studies, they also introduce new innovations that advance the state-of-the-art in network optimization techniques for IoT applications.

4.4. Analysis of experimental results

In order to assess how well the suggested approach and S·P·S method perform, this study chooses four important metrics: CPU utilization, message overhead, network traffic consumption, and path convergence time. The entire amount of traffic used by the ground network to send packets throughout the test period is known as network traffic consumption. The total number of routing messages announced by the terrestrial network during the test period is referred to as message overhead.

4.4.1. CPU use and path convergence time

In a small-scale network context, the path convergence time and CPU consumption are displayed in Figs. 9 and 10, respectively. By re-establishing the neighbor relationship, border routers using the proposed method accelerate route convergence by not transmitting historical routing information. Furthermore, a significant decrease in the quantity of packets delivered results in a corresponding decrease in CPU consumption. The test results demonstrate that the suggested strategy reduces CPU use by 7.18 %–8.40 % and path convergence time by 610 ms–720 ms when compared to the S·P·S method.

4.4.2. Traffic consumption

Traffic consumption is a significant overhead indicator since it uses up the earth station's bandwidth resources when all routing prefix messages are announced. Fig. 11 displays the bandwidth resources used by ground station G1 to send routing messages. The bandwidth cost of the suggested solution is only 41 % of the initial cost when 20,000 route prefixes are published and the topology is changed four times. Fig. 12 displays the total amount of update messages that ground station G1 has announced. The number of updated messages in the suggested way is only 35 % of the original messages in the test situation when the topology changes four times.

As part of the ongoing assessments, we measured and sampled a portion of bandwidth in three rounds for a size of 128 kbps. Sending packets and concurrently moving data within 60 s is how bandwidth is used. Table 5 shows that, for the first measurement, there were 3.102 packages. Using the S·P.S. approach, the average success rate of package reduction for measurements 1 through 3 was 61.22 %, which is not the same as the way that is suggested for determining the success rate of package reduction. has been 72.63 %; similarly, the proposed method has outperformed the S·P·S method in all three measures on average for the amount of traffic reduction and energy consumption, so that the proposed method has outperformed the similar method for the 10 % traffic reduction and the 9 % energy consumption.

5. Conclusion

This research presents a novel approach to optimizing the utilization of the Border Gateway Protocol (BGP) in Internet of Things (IoT) networks, specifically focusing on multi-temporal networks involving sensor nodes. Through the development and implementation of the Critical Information Aggregation and Scheduling Method (CSAM), we address the challenge of reducing the overhead and energy consumption related to the transmission of small and medium packets in such networks. The findings of this study demonstrate that CSAM effectively mitigates the overhead introduced by the BGP protocol stack, leading to significant reductions in network traffic and energy consumption. By scheduling and aggregating BGP packets at sensor nodes, prioritizing packet transmission, and managing message scheduling, CSAM optimizes network performance while maintaining the integrity of the underlying protocol stack. Empirical evaluations have confirmed the effectiveness of CSAM, with tangible improvements observed in CPU utilization, path convergence time, and traffic consumption compared to standard methods. Overall, the findings highlight the potential of CSAM to enhance the scalability and efficiency of IoT networks, particularly in applications requiring periodic monitoring and data transmission.

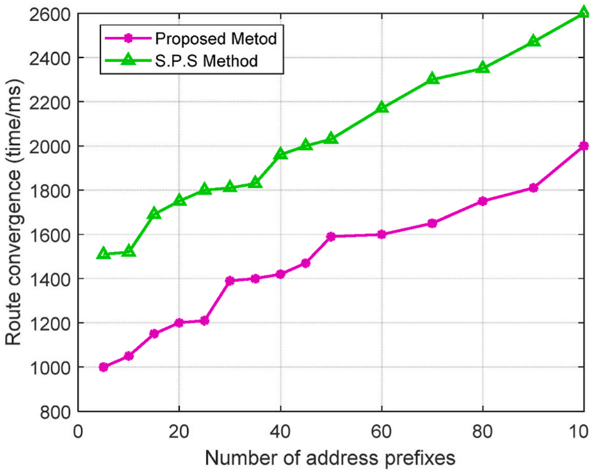


Fig. 9. Comparison of convergence times.

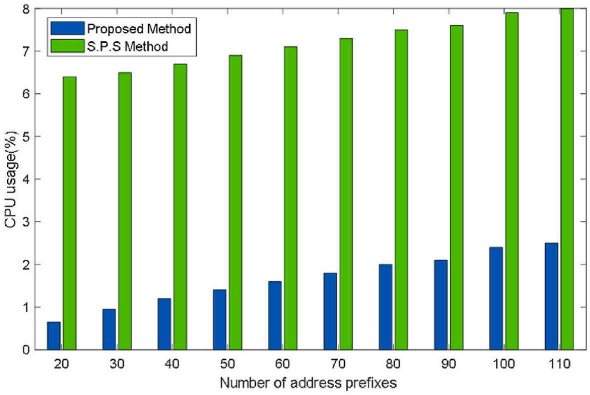


Fig. 10. Comparison of CPU usage.

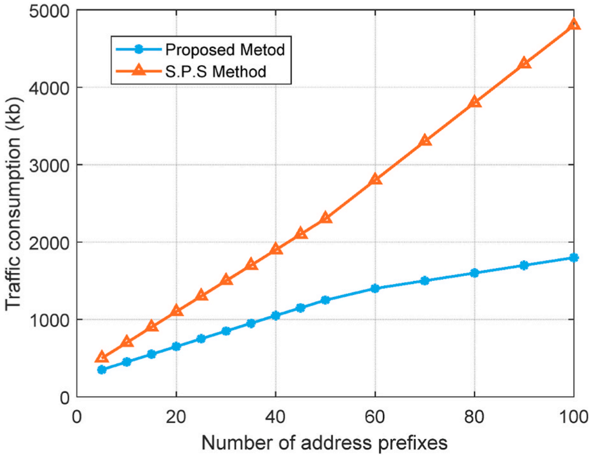


Fig. 11. Comparison of bandwidth use.

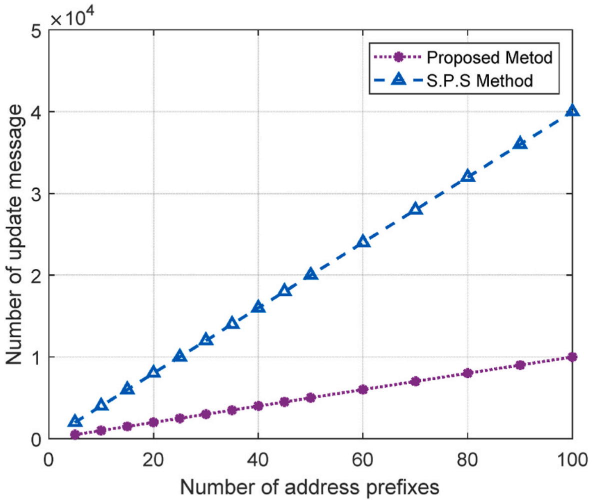


Fig. 12. Comparison of message overhead.

Table 5
Sampling results for 128 Kb bandwidth.

Methods	Measurements	Packets	Success rate in reducing outgoing packets (%)	amount of traffic reduction (%)	Energy consumption rate reduction (%)
S·P·S Method	1	3.102	63.01	75.30	18.34
	2		61.23	74.62	17.82
	3		59.42	71.36	17.02
Proposed Method	1	3.102	74.51	85.90	26.31
	2		73.29	83.40	25.79
	3		70.10	82.12	25.15

Moving forward, several avenues for future research and development in this area are proposed. Firstly, further investigation is needed to explore the potential integration of CSAM with other optimization techniques and protocols to achieve even greater efficiency gains in IoT networks. Additionally, exploring the potential impacts of CSAM on network security and resilience will be crucial for ensuring the robustness of IoT deployments. Lastly, efforts to standardize and disseminate CSAM methodologies and best practices within the research and practitioner communities will be essential for facilitating the widespread adoption and deployment of this optimization approach. By addressing these research directions, we aim to make further progress in Internet of Things network optimization and help realize efficient, scalable, and sustainable IoT ecosystems.

Ethics statement

Ethics committee review and/or approval was not required for this study, as no animal or human-based experiments/case studies were used.

Data availability statement

The authors do not have permission to share data.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Meng Yan: Visualization, Validation, Resources, Methodology, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Science and Technology Research Project of Education Department of Jilin Province; Project name: Development of VR - based multi - machine asynchronous distribution management cloud platform system, Project number: JJKH20231460KJ.

References

[1] E. Ramadhan, A. Firdausi, S. Budiyanto, Design and analysis QoS VoIP using routing border gateway protocol (BGP), in: 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), IEEE, 2017, November, pp. 1–4.
[2] Singh, M., & Malik, A. Multi-hop routing protocol in SDN-based wireless sensor network: a comprehensive survey. Software-Defined Network Frameworks, 121-141.
[3] A.K. Lodhi, M.S.S. Rukmini, S. Abdulsattar, Energy-efficient routing protocol for network life enhancement in wireless sensor networks, Recent Advances in Computer Science and Communications (Formerly: Recent Pat. Comput. Sci. 14 (3) (2021) 864–873.
[4] C. Meng, H. Motevalli, Link prediction in social networks using hyper-motif representation on hypergraph, Multimed. Syst. 30 (3) (2024) 123.
[5] M.F. Km, N. Santhiyakumari, 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, February, pp. 1361–1367.
[6] Xiangjun Wu, Shuo Ding, Ning Xu, Ben Niu, Periodic Event-Triggered Bipartite ContainmentControl for Nonlinear Multi-Agent Systems With luput Delay, Int. J. Syst. Sci. (2024). https://doi.org/10.1080/00207721.2024.2328780.
[7] X. Zhao, S.S. Band, S. Elnaffar, M. Sookhak, A. Mosavi, E. Salwana, The implementation of border gateway protocol using software-defined networks: a systematic literature review, IEEE Access 9 (2021) 112596–112606.
[8] P. Wang, S. Xia, H. Wang, X. Xu, A lightweight management protocol for IPv6-based wireless sensor networks, in: 2015 Chinese Automation Congress (CAC), IEEE, 2015, November, pp. 1143–1148.
[9] L. Zhang, S. Hu, M. Trik, S. Liang, D. Li, M2M communication performance for a noisy channel based on latency-aware source-based LTE network measurements, Alex. Eng. J. 99 (2024) 47–63.

[10] Shuihui Liu, Huanqing Wang, Yunfeng Liu, Ning Xu, Xudong Zhao, Sliding-mode surface-based adaptive optimal nonzero-sum games for saturated nonlinear multi-player systems with identifier-critic networks, Neurocomputing 584 (2024) 127575, https://doi.org/10.1016/j.neucom.2024.127575.

[11] Heng Zhao, Ning Zhao, Guangdeng Zong, Xudong Zhao, Ning Xu, Sliding-mode surface-based approximate optimal control for nonlinear multiplayer Stackelberg-Nash games via adaptive dynamic programming, Commun. Nonlinear Sci. Numer. Simulat. 132 (2024) 107928.

[12] M. Trik, H. Akhavan, A.M. Bidgoli, A.M.N.G. Molk, H. Vashani, S.P. Mozaffari, A new adaptive selection strategy for reducing latency in networks on chip, Integration 89 (2023) 9–24.

[13] Ning Xu, Liu Xiang, Yulin Li, Guangdeng Zong, Xudong Zhao, Dynamic event-triggered control for a class of uncertain strict-feedback systems via an improved adaptive neural networks backstepping approach, IEEE Trans. Autom. Sci. Eng. (2024), https://doi.org/10.1109/TASE.2024.3374522.

[14] J. Sun, Y. Zhang, M. Trik, PBPHS: a profile-based predictive handover strategy for 5G networks, Cybern. Syst. (2022) 1–22.

[15] Sai Huang, Ben Niu, Huanqing Wang, Ning Xu, Xudong Zhao, Prescribed performance-based low-complexity adaptive 2-bit-triggered control for unknown nonlinear systems with actuator dead-zone, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS 71 (2) (2024) 762–766.

[16] Z. Wang, Z. Jin, Z. Yang, W. Zhao, 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 35 (9) (2023) 101732.

[17] Haoyu Zhang, Quan Zou, Ying Ju, Chenggang Song, Dong Chen, Distance-based support vector machine to predict DNA N6-methyladine modification, Curr. Bioinf. 17 (5) (2022) 473–482.

[18] E. Khezri, R.O. Yahya, H. Hassanzadeh, M. Mohaidat, S. Ahmadi, M. Trik, DLJSF: data-locality aware job scheduling IoT tasks in fog-cloud computing environments, Results in Engineering 21 (2024) 101780.

[19] Chen Cao, Jianhua Wang, Devin Kwok, Zilong Zhang, Feifei Cui, Da Zhao, Mulin Jun Li, Quan Zou, webTWAS: a resource for disease candidate susceptibility genes identified by transcriptome-wide association study, Nucleic Acids Res. 50 (D1) (2022) D1123–D1130.

[20] G. Wang, J. Wu, M. Trik, A novel approach to reduce video traffic based on understanding user demand and D2D communication in 5G networks, IETE J. Res. (2023) 1–17.

[21] Zhen Gao, Ning Zhao, Xudong Zhao, Ben NiuNing, Event-triggered prescribed performance adaptive secure control fornonlinear cyber physical systems under denial-of-service attacks, Commun. Nonlinear Sci. Numer. Simulat. 131 (2024) 107793, https://doi.org/10.1016/j.cnsns.2023.10.

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

[23] Shihui Liu, Ben Niu, Ning Xu, Xudong Zhao, Zero-sum game-based decentralized optimal control for saturated nonlinear interconnected systems via a data and event driven approach, IEEE Syst. J. (2024), https://doi.org/10.1109/JSYST.2024.3350771.

[24] L. Zhang, S. Hu, M. Trik, S. Liang, D. Li, M2M communication performance for a noisy channel based on latency-aware source-based LTE network measurements, Alex. Eng. J. 99 (2024) 47–63.

[25] F. Yin, Z. Lin, Q. Kong, Y. Xu, D. Li, S. Theodoridis, S.R. Cui, FedLoc: federated learning framework for data-driven cooperative localization and location data processing, IEEE Open Journal of Signal Processing 1 (2020) 187–215, https://doi.org/10.1109/OJSP.2020.3036276.

[26] N. Aljojo, Network transmission flags data affinity-based classification by K-nearest neighbor, Aro-The Scientific Journal of Koya University 10 (1) (2022) 35–43.

[27] F. Yin, C. Fritsche, D. Jin, F. Gustafsson, A.M. Zoubir, Cooperative localization in WSNs using Gaussian mixture modeling: distributed ECM algorithms, IEEE Trans. Signal Process. 63 (6) (2015) 1448–1463, https://doi.org/10.1109/TSP.2015.2394300.

[28] G. Sun, Z. Xu, H. Yu, X. Chen, V. Chang, A.V. Vasilakos, Low-latency and resource-efficient service function chaining orchestration in network function virtualization, IEEE Internet Things J. 7 (7) (2020) 5760–5772, https://doi.org/10.1109/JIOT.2019.2937110.

[29] S. Mala, S.V. Mallapur, A brief analysis of border gateway protocol for internet controlling and malicious attacks, in: International Conference on Computing, Communication, Electrical and Biomedical Systems, Springer International Publishing, Cham, 2022, February, pp. 561–572.

[30] P.J.M. Ali, Investigating the Impact of min-max data normalization on the regression performance of K-nearest neighbor with different similarity measurements, ARO-The Scientific Journal of Koya University 10 (1) (2022) 85–91.

[31] G. Sun, G. Zhu, D. Liao, H. Yu, X. Du, M. Guizani, Cost-efficient service function chain orchestration for low-latency applications in NFV networks, IEEE Syst. J. 13 (4) (2019) 3877–3888, https://doi.org/10.1109/JSYST.2018.2879883.

[32] G. Sun, Y. Li, D. Liao, V. Chang, Service function chain orchestration across multiple domains: a full mesh aggregation approach, IEEE Transactions on Network and Service Management 15 (3) (2018) 1175–1191, https://doi.org/10.1109/TNSM.2018.2861717.

[33] A. Agarwal, S. Sharma, Performance evaluation of hsrp, glbp and vrrp with interior gateway routing protocol and exterior gateway routing protocol, in: 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, 2022, January, pp. 153–158.

[34] N.A. Hussein, Synchro software-based alternatives for improving traffic operations at signalized intersections, aro-the scientific journal of koya university 10 (1) (2022) 123–131.

[35] X. Xu, W. Liu, L. Yu, Trajectory prediction for heterogeneous traffic-agents using knowledge correction data-driven model, Inf. Sci. 608 (2022) 375–391, https://doi.org/10.1016/j.ins.2022.06.073.

[36] B. Ma, Z. Liu, Q. Dang, W. Zhao, J. Wang, Y. Cheng, Z. Yuan, Deep reinforcement learning of UAV tracking control under wind disturbances environments, IEEE Trans. Instrum. Meas. 72 (2023) 1–13, https://doi.org/10.1109/TIM.2023.3265741.

[37] T.L. Narayana, C. Venkatesh, A. Kiran, A. Kumar, S.B. Khan, A. Almusharraf, M.T. Quasim, Advances in real time smart monitoring of environmental parameters using IoT and sensors, Heliyon 10 (7) (2024) E28195.

[38] A.H. Taher, Train support vector machine using fuzzy C-means without a prior knowledge for hyperspectral image content classification, aro-the scientific journal of koya university 10 (2) (2022) 22–28.

[39] D. Khan, M. Alonazi, M. Abdelhaq, N. Al Mudawi, A. Algarni, A. Jalal, H. Liu, Robust human locomotion and localization activity recognition over multisensory, Front. Physiol. 15 (2024), https://doi.org/10.3389/fphys.2024.1344887.

[40] K. Li, L. Ji, S. Yang, H. Li, X. Liao, Couple-group consensus of cooperative–competitive heterogeneous multiagent systems: a fully distributed event-triggered and pinning control method, IEEE Trans. Cybern. 52 (6) (2022) 4907–4915, https://doi.org/10.1109/TCYB.2020.3024551.

[41] B. Chen, J. Hu, Y. Zhao, B.K. Ghosh, Finite-time velocity-free rendezvous control of multiple AUV systems with intermittent communication, IEEE Transactions on Systems, Man, and Cybernetics: Systems 52 (10) (2022) 6618–6629, https://doi.org/10.1109/TSMC.2022.3148295.

[42] L. Zhao, S. Qu, H. Xu, Z. Wei, C. Zhang, Energy-efficient trajectory design for secure SWIPT systems assisted by UAV-IRS, Vehicular Communications 45 (2024) 100725, https://doi.org/10.1016/j.vehcom.2023.100725.

[43] Q. Liao, H. Chai, H. Han, X. Zhang, X. Wang, W. Xia, Y. Ding, An integrated multi-task model for fake news detection, IEEE Trans. Knowl. Data Eng. 34 (11) (2022) 5154–5165, https://doi.org/10.1109/TKDE.2021.3054993.

[44] M. Hou, Y. Zhao, X. Ge, Optimal scheduling of the plug-in electric vehicles aggregator energy and regulation services based on grid to vehicle, International Transactions on Electrical Energy Systems 27 (6) (2017) e2364, https://doi.org/10.1002/etep.2364.

[45] F. Ouakasse, S. Rakrak, A comparative study of MQTT and COAP application layer protocols via. performances evaluation, J. Eng. Appl. Sci. 13 (15) (2018) 6053–6061.

[46] J. Zhang, J. Ren, Y. Cui, D. Fu, J. Cong, Multi-USV task planning method based on improved deep reinforcement learning, IEEE Internet Things J. (2024), https://doi.org/10.1109/JIOT.2024.3363044.

[47] H.A. Ahmed, P.J.M. Ali, A.K. Faeq, S.M. Abdullah, An investigation on disparity responds of machine learning algorithms to data normalization method, aro-the scientific journal of koya university 10 (2) (2022) 29–37.

[48] J. Li, J. Li, C. Wang, F.J. Verbeek, T. Schultz, H. Liu, MS2OD: outlier detection using minimum spanning tree and medoid selection, Mach. Learn.: Sci. Technol. 5 (1) (2024) 15025, https://doi.org/10.1088/2632-2153/ad2492.

[49] H. Han, J. Tang, Z. Jing, Wireless sensor network routing optimization based on improved ant colony algorithm in the Internet of Things, Heliyon 10 (1) (2024) e23577.

[50] T.S. Othman, S.M. Abdullah, An intelligent intrusion detection system for internet of things attack detection and identification using machine learning, aro-the scientific journal of koya university 11 (1) (2023) 126–137.

[51] J. Luo, C. Zhao, Q. Chen, G. Li, Using deep belief network to construct the agricultural information system based on Internet of Things, J. Supercomput. 78 (1) (2022) 379–405, https://doi.org/10.1007/s11227-021-03898-y.

[52] H. Jiang, Z. Xiao, Z. Li, J. Xu, F. Zeng, D. Wang, An energy-efficient framework for internet of things underlaying heterogeneous small cell networks, IEEE Trans. Mobile Comput. 21 (1) (2022) 31–43, https://doi.org/10.1109/TMC.2020.3005908.

[53] Y.A. Hassan, A.M.S. Rahma, The most common characteristics of fragile video watermarking, ARO-The Scientific Journal of Koya University 11 (1) (2023) 99–104.

[54] Z. Xiao, H. Fang, H. Jiang, J. Bai, V. Havyarimana, H. Chen, L. Jiao, Understanding private car aggregation effect via spatio-temporal analysis of trajectory data, IEEE Trans. Cybern. 53 (4) (2023) 2346–2357, https://doi.org/10.1109/TCYB.2021.3117705.

[55] H. Jiang, S. Chen, Z. Xiao, J. Hu, J. Liu, S. Dustdar, Pa-count: passenger counting in vehicles using wi-fi signals, IEEE Trans. Mobile Comput. (2023), https://doi.org/10.1109/TMC.2023.3263229.

[56] L. Nouri, S.I. Yahya, A. Rezaei, F.A. Hazzazi, B.N. Nhu, A compact negative group delay microstrip diplexer with low losses for 5G applications, aro-the scientific journal of koya university 11 (2) (2023) 17–24.

[57] B. Cao, J. Zhao, P. Yang, Y. Gu, K. Muhammad, J.J.P.C. Rodrigues, V.H.C. de Albuquerque, Multiobjective 3-D topology optimization of next-generation wireless data center network, IEEE Trans. Ind. Inf. 16 (5) (2020) 3597–3605, https://doi.org/10.1109/TII.2019.2952565.

[58] M.A. Pirdawood, S.R. Kareem, D.C. Zahir, Audio encryption framework using the laplace transformation, aro-the scientific journal of koya university 11 (2) (2023) 31–37.

[59] W. Zheng, P. Deng, K. Gui, X. Wu, An Abstract Syntax Tree based static fuzzing mutation for vulnerability evolution analysis, Inf. Software Technol. (2023) 107194, https://doi.org/10.1016/j.infsof.2023.107194.

[60] M.F. Sabri, Investigating and studying the modifications of nano and micro-sized amorphous materials under the influence of a high energy radiation, aro-the scientific journal of koya university 11 (2) (2023) 73–82.

[61] J. Hu, Y. Wu, T. Li, B.K. Ghosh, Consensus control of general linear multiagent systems with antagonistic interactions and communication noises, IEEE Trans. Automat. Control 64 (5) (2019) 2122–2127, https://doi.org/10.1109/TAC.2018.2872197.

[62] S.B. Neamah, A.A. Karim, Real-time traffic monitoring system based on deep learning and YOLOv8, aro-the scientific journal of koya university 11 (2) (2023) 137–150.

[63] Q. Wang, J. Hu, Y. Wu, Y. Zhao, Output synchronization of wide-area heterogeneous multi-agent systems over intermittent clustered networks, Inf. Sci. 619 (2023) 263–275, https://doi.org/10.1016/j.ins.2022.11.035.

[64] S. Roshani, S.I. Yahya, Y.Y. Ghadi, S. Roshani, F. Parandin, B.D. Yaghouti, Size reduction and harmonics suppression in microwave power dividers, aro-the scientific journal of koya university 11 (2) (2023) 122–136.

[65] Y. Jiang, X. Li, Broadband cancellation method in an adaptive co-site interference cancellation system, Int. J. Electron. 109 (5) (2022) 854–874, https://doi.org/10.1080/00207217.2021.1941295.

[66] X. Zhang, H. Deng, Z. Xiong, Y. Liu, Y. Rao, Y. Lyu, Y. Li, Secure routing strategy based on attribute-based trust access control in social-aware networks, Journal of Signal Processing Systems (2024), https://doi.org/10.1007/s11265-023-01908-1.

[67] J. Mou, K. Gao, P. Duan, J. Li, A. Garg, R. Sharma, A machine learning approach for energy-efficient intelligent transportation scheduling problem in a real-world dynamic circumstances, IEEE Trans. Intell. Transport. Syst. 24 (12) (2023) 15527–15539, https://doi.org/10.1109/TITS.2022.3183215.

[68] Y. Ding, W. Zhang, X. Zhou, Q. Liao, Q. Luo, L.M. Ni, FraudTrip: taxi fraudulent trip detection from corresponding trajectories, IEEE Internet Things J. 8 (16) (2021) 12505–12517, https://doi.org/10.1109/JIOT.2020.3019398.

[69] G. Liu, Data collection in MI-assisted wireless powered underground sensor networks: directions, recent advances, and challenges, IEEE Commun. Mag. 59 (4) (April 2021) 132–138, https://doi.org/10.1109/MCOM.001.2000921.

[70] Z. Wu, H. Zhu, L. He, Q. Zhao, J. Shi, W. Wu, Real-time stereo matching with high accuracy via Spatial Attention-Guided Upsampling, Appl. Intell. 53 (20) (2023) 24253–24274, https://doi.org/10.1007/s10489-023-04646-w.

[71] W. Wu, H. Zhu, S. Yu, J. Shi, Stereo matching with fusing adaptive support weights, IEEE Access 7 (2019) 61960–61974, https://doi.org/10.1109/ACCESS.2019.2916035.

[72] Z.U. Khan, Q. Gang, A. Muhammad, M. Muzzammil, S.U. Khan, M.E. Affendi, J. Khan, A comprehensive survey of energy-efficient MAC and routing protocols for underwater wireless sensor networks, Electronics 11 (19) (2022) 3015.

[73] A. Ahmed, S. Jabbar, M.M. Iqbal, M. Ibrar, A. Erbad, H. Song, An efficient hierarchical mobile IPv6 group-based BU scheme for mobile nodes in IoT network, IEEE Internet Things J. 10 (10) (2022) 8684–8695.