# Credit-Based Shaping As Defense Against DoS Attacks

Leonard Nolting, Florian Wiedner*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: leonard.nolting@tum.de, wiedner@net.in.tum.de

***Abstract*—Time-Sensitive Networking (TSN) is a frequently researched alternative for real-time Ethernet networks using time-synchronization, shaping, scheduling and more techniques to accommodate streams with different latency and bandwidth requirements on one network. The Credit-Based Shaper (CBS) awards credits to queues at a linear rate, limiting their bandwidth and controlling the burstiness of traffic.**

**As Denial-of-Service (DoS) attacks remain relevant and TSN networks often are used in critical cyber-physical systems, the defense capabilities of TSN networks against DoS attacks need to be evaluated.**

**We explore how well CBS can protect TSN networks from DoS attacks by assessing the possible scenarios and categorizing attacks with a DoS taxonomy. We will find that CBS can by no means replace proper security mechanisms, but in certain scenarios can protect large parts of a TSN network from an attack, especially when the attacker can only send in the best-effort traffic class.**

***Index Terms*—denial-of-service, time-sensitive networking, credit-based shaper, security**

## 1. Introduction

Best-effort traffic delivers "most packets, most of the time, mostly in order" [1]. It lacks determinism. Applications that require tighter guarantees by their network, such as industrial control, electrical grids or in-vehicle networks, traditionally created domain-specific solutions, for example EtherCAT, PROFINET or CAN [1]–[4].

Time-Sensitive Networking (TSN) is a set of standards that enable such guarantees for standard Ethernet by providing upper bounds on latency and decreasing packet loss. They are maintained by the IEEE 802.1 working group. Among others, TSN is "promising to replace existing protocols in mission-critical domains" [5], where correct timing not only affects performance but also safety and security.

The growing adoption of TSN, combined with its extreme susceptibility to traffic disruptions and the vulnerability of the domains it is employed in, raises questions about the protocol's security. The European Union Agency for Cybersecurity finds Denial-of-Service (DoS) attacks "ranked at the top during the reporting period for another year" [6], especially "on the critical infrastructures of countries" [7].

As TSN is still young and in the standardization phase, its security aspect has been researched significantly less than more established systems like Ethernet, IP or alternative real-time protocols. Several papers look specifically at IEEE 802.1Qci "Per-Stream Filtering and Policing" [8], [9]. The security of TSN in general is considered by Ergenç et al. [5], others focus on specific domains [2], [10]–[12]. Furthermore, building upon the Credit-Based Shaper (CBS), Meyer et al. propose Credit-Based Metering [13].

IEEE 802.1Q describes the Credit-Based Shaper (CBS), which limits the bandwidth of a traffic class by only awarding it a certain amount of credit over time. Using CBS shaping can potentially mitigate DoS attacks on TSN networks, but this has not yet been evaluated.

In this paper, we explore the strengths and limitations of using CBS without modifications to defend against varying types of DoS attacks.

We will first cover the underlying technological aspects, as well as DoS attack vectors on TSN networks. This will be followed by an evaluation and a clear compilation of the results, including suggestions for follow-up research.

## 2. Background

The paper combines several topics, which will be briefly summarized in the following subsections.

### Time-Sensitive Networking

TSN is a feature offered by a network that simultaneously hosts regular best-effort traffic.

All TSN nodes synchronize their clocks on the network. TSN flows represent a contract between the network and the end hosts about bandwidth, latency, jitter and packet loss, and can be created and ended flexibly. It aims to eliminate congestion loss completely by controlling the traffic shape and schedule. Shaping limits bandwidth and smooths out traffic, whereas scheduling determines when packets are sent from a queue. TSN provides several algorithms for that. See [1] for a good in-depth introduction. In this paper, we will inspect the CBS.

### Credit-Based Shaper

Traffic shaping creates gaps between packets [3]. This may seem counterintuitive to latency goals, but it gives other flows a chance to find a gap in a burst of packets, essentially skipping the queue which is full from the burst. For a minimal illustrative example, see [3].

One switch can have multiple CBS shaped queues per egress port. For each, a credit value is stored, starting at

 doi: 10.2313/NET-2025-11-3_06

zero. When a packet from that queue is sent, the credit value is reduced by the length of the packet. Now, credit replenishes at a set rate called `idleSlope` until it reaches zero. Only once it is back to zero, the queue may be eligible again, meaning it is ready to send.

If the queue is eligible but cannot send because the transmitter is currently occupied by another queue, this is the first time credits accumulate over zero. The queue can now send packets as long as its credit stays greater than or equal to zero, and it is nonempty. Once it empties but still has credit left, it is reset to zero.

Helpful visualizations and more detailed explanations can be found in [3].

### Types of DoS attacks

A DoS attack is "an attempt to make a computer resource unavailable to its intended users." [14]. This general goal can be achieved in many ways, e.g. a physical attack on a facility. In order to limit the scope of this paper, we will only look at attacks performed through means of a network connection.

Over time, many attack and prevention mechanism categorizations for such DoS attacks have been published, such as by Karig and Lee [15], Fadlallah and Serhrouchni [16], Specht and Lee [17], Douligeris and Mitrokotsa [18] and Mirkovic and Reiher [19], some of which are more detailed than others. This paper is based on a later taxonomy by Ramanauskaite and Cenys [14] that reviews and combines the previous mentions into one.

DoS attacks vary significantly in nature and can be classified in multiple dimensions. Understanding this taxonomy is important for analyzing the effectiveness of CBS as a defense mechanism in TSN, which will be done in Section 4.

One main classification is based on the number of sources involved in the attack:

- **Single Source Attack**: DoS attack launched from a single machine
- **Distributed Denial-of-Service (DDoS) Attack**: coordinated DoS attack launched from multiple systems

Another dimension considers the vulnerability exploited:

- **Bug Exploitation Attack**: exploits software or hardware vulnerabilities in the victim's system to cause a denial-of-service
- **Resource Depletion Attack**: consumes a system's resources, making them unavailable for legitimate requests:
  - **Memory Depletion Attack**: fills up the system's memory
  - **CPU Work Depletion Attack**: overloads the system's CPU by requiring it to perform excessive processing
  - **Semantic Resource Depletion Attack**: exploits modified incoming packets to consume more resources
- **Bandwidth Exhaustion Attack**: floods the target with a large amount of data, consuming all available network bandwidth and preventing legitimate traffic from reaching the victim

These dimensions, along with a dimension distinguishing single nodes or the network being affected, are visualized in Figure 1.

In the context of Time-Sensitive Networks, the most relevant types of DoS attacks are resource depletion attacks and bandwidth exhaustion attacks. These attacks can directly impact the network's ability to deliver time-sensitive data, which can cause missed deadlines in real-time applications.

In the following sections of this paper, we will explore whether Credit-Based Shaping can be employed to counteract these attacks in Time-Sensitive Networks. First, we will look at the methodology used to analyze this topic.

## 3. Context

The purpose of this paper is to find out when CBS can be used to mitigate DoS attacks.

It is critical to understand why and how DoS attacks affect TSN networks, first. For that, we will now evaluate the relevance of DoS attacks for TSN networks and which scenarios that would affect. After that, we will cover existing security mechanisms in TSN. Finally, the evaluation and conclusion will follow in Sections 4 and 5.

### Understanding DoS Applicability in TSN networks

TSN often operates in isolated networks and security benefits from that, as attackers need to gain access to the network first before they can start a DoS attack [1], [20]. One might wonder how DoS attacks are relevant to the typical network that employs TSN at all.

First, a device within the network could be infected over other means than a network connection, for example through a bad update. The infected node could then cause a DoS attack. This shows that isolation cannot be a full security guarantee and does not serve as reliable protection. Isolated networks therefore are not immune to DoS attacks and estimating their potential impact and countermeasures is still relevant.

Additionally, with the shift of TSN towards being used for routed networks, such as with DetNet, TSN networks are increasingly losing their isolation property as they are being connected to wide area networks. This increases the risk of attacks and lowers the barrier for potential attackers, especially from remote locations [1], [21].

Furthermore, the use-cases for Operational Technology (OT) networks and TSN significantly overlap [1], [4], [10], [22], and with the convergence of OT and IT networks come "cyber security challenges that are typically associated with only with IT infrastructures" [20], [21]

Due to the time-sensitive and cyber-physical nature of TSN networks, they "present potentially attractive targets for cyber attackers" [21].

An additional consideration is that real-time systems like TSN will often employ embedded microcontrollers with little resources, making them sensitive to even small attacks.

This provides context about why DoS attacks are relevant to TSN networks and under which circumstances they occur.

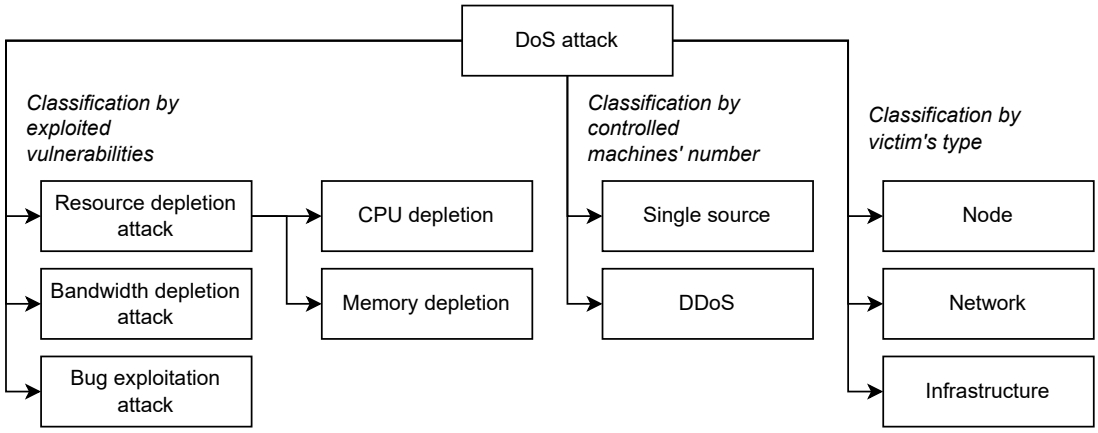


Figure 1: An adjusted version of the taxonomy suggested in [14].

### Existing security mechanisms in TSN

TSN standards primarily focus on the key characteristics (performance, determinism) and practicality/ease-of-use. Security is not a core consideration and has to be actively added [5].

Existing network security paradigms, such as firewalls, traffic anomaly detection or authentication can be used with TSN, but may have to be adapted to the timing requirements by TSN [1], [5].

Additionally, the IEEE provides several proposed or standardized security mechanisms such as “Per-stream filtering and policing”, “Frame Replication and Elimination for Reliability” or “MACsec” [5], [23].

However, to isolate the effects that CBS has on security, we will consider a network implementation with CBS alone and no optional standards.

## 4. Evaluation

We will now assess the effect of CBS on security in TSN networks against DoS attacks based on the structure given by the DoS taxonomy discussed in Section 2.

In general, TSN and CBS greatly increase the complexity of a network, increasing the attack surface for semantic DoS attacks [19] / bug exploitation attacks [14]. Since CBS does not examine packet contents, it has no impact on the defense against this type of attack.

### Attacker Inside the Network

As stated in Section 3, a DoS attack can occur in an isolated network from a node inside the network itself, if it has previously been infected.

This can lead to a special case, where if the infected node itself represents a service, its denial can be caused by it not sending any packets. In the DoS taxonomy, this is represented as “Denial of Node”. As CBS never goes into effect here for the lack of packets, it cannot stop this attack.

Otherwise, a DoS can only be achieved through sending many or malformed packets.

When a node sends too many packets through an existing flow, it will fill the queue of the switch it is connected to (for end devices the ingress switch). Since CBS does not allocate an individual queue to each flow, other flows sharing the same queue will be starved of buffer space. That is a Memory Depletion Attack, which can lead to significant congestion loss through buffer overflows. As TSN under normal operation eliminates congestion loss completely, the starved nodes might not know how to react to that, causing unpredictable errors [1]. For example, in combination with TSN Frame Replication and Elimination, a network can assume zero packet loss and might consider a node as faulty when its packets are not received. This leads to the perceived failure of entire nodes, virtually taking down entire machines.

Additionally, credit is only allocated per CBS-queue, thus other flows will be starved of credit as well, resulting in a perceived Bandwidth Depletion Attack [3].

CBS can only limit the starvation to the traffic class of the attacking flow and any lower priority classes, as that is the granularity of its queues and credits. Hence, higher priority traffic is protected from this type of attack, while lower priority traffic, such as best-effort, is not specially protected.

A sender might also send an amount of packets which overloads the classification algorithm of the receiving switch, causing a CPU work depletion attack, or more generally, if offloaded, a processing work depletion attack. This can cause the failure of the entire switch. Since shaping is performed after classification, the CBS shaper cannot stop that type of attack.

On the physical level, since Ethernet is a shared medium, an attacking node can deplete nodes also connected to its outgoing ports by sending excessive amounts of packets, provoking collisions. This bandwidth depletion attack also happens in front of shapers, hence CBS cannot prevent this.

So far, we assumed the attacking node only uses existing flows and their traffic classes. If it can create flows of arbitrary classes, with enough bandwidth, it can overload all queues of a port at the same time, which starves all other flows routed on that port of bandwidth and causes unexpected congestion loss. In this case, CBS cannot mitigate the DoS attack and the entire port fails.

If the attacker also sends to varying destination addresses which are routed on different egress ports of the

 doi: 10.2313/NET-2025-11-3_06

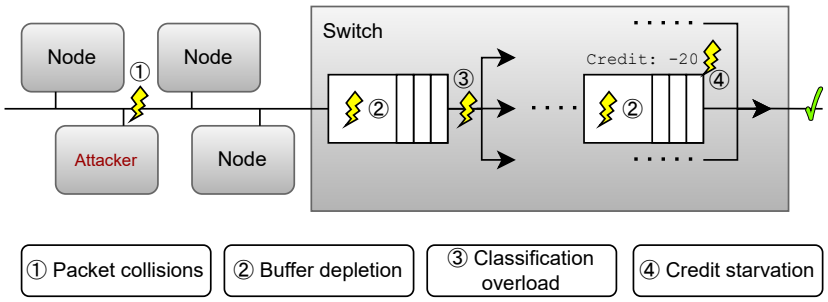


Figure 2: A simplified illustration of possible brute-force vulnerabilities with one attacking node inside the network.

same or different switches, it can multiply its effect across all egress port of all switches it is connected to.

As multiple nodes get involved, forming a DDoS attack, each node can attack in above fashion, denying the service of all switches that each attacker is connected to in the worst case.

### Attacker Outside the Network

If the attacker is outside the TSN domain, it is most likely switched as best-effort IP traffic. Reference [1] states as an essential feature of TSN that the best-effort traffic class can employ all the usual tools for IP traffic, so the mitigation of DoS attacks can be handled by these. However, since credits are only given to CBS-queues and CBS traffic has higher priority than best-effort traffic, it is protected from bandwidth starvation even in the event of a DoS attack from best-effort traffic. If the outside machine is equipped with the necessary hardware and no security mechanisms are in place, it can also create CBS flows, essentially making it a part of the TSN domain. The above evaluation for an inside attacker applies.

### After the Ingress Bridge

The CBS shaper forwards packets at a "rate such that, over a relatively short term, is equal to the total bandwidth allocated to the TSN flows using that queue" [1]. Bandwidth and burstiness are predictable and controlled, even in the event of a DoS attack. This leads to any DoS attack being contained to the connected ingress switches and all their nodes. It will not propagate further into the network, defending it against the attack.

Bandwidth and burstiness depend on the single parameter `idleSlope` that is passed to CBS-queues. As the network accounts for the queue behavior derived from the parameter, changes to it have no effect on the outcome [24].

Less resource-intensive pulsing attacks, with the goal of transmitting packets exactly when credits replenish, do not work, since CBS-queues are first-come, first-serve (FIFO) [3], [24].

A low and slow attack of creating many flows cannot specifically target the CBS, since it does not keep state or allocate computing resources for each flow.

As by design of CBS, it is also not possible to provoke one node to accumulate a very high credit number through blocking a port and subsequently a queue for a long time. CBS defines a `hiCredit` value, limiting the maximum amount of credits a queue can reach, which is taken into consideration for bandwidth and burstiness calculations [24].

## 5. Conclusion and Future Work

In this paper, we analyzed to which extent and with which constraints CBS can defend against DoS attacks. The core finding is that behind CBS shaped queues, the network is safe from brute-force attacks. Furthermore, CBS as a security mechanism works better the more restricted the access is that each node has to other ports and queues. However, the evaluation also clearly shows that CBS is by no means a complete tool against DoS attacks. Its most obvious shortcoming are semantic attacks, which it cannot detect and protect of and where it consequently cannot replace additional security tools, such as Intrusion Detection Systems. It is important to be aware it was not designed for security purposes and should not be advertised as a solution.

For more certainty about the positive results in this paper, future work needs to verify the results in both network simulators and real networks. In order to reduce the impact of DoS attacks, future work could explore introducing traffic class checks and destination checks at switches. Switches will check if the sender of an incoming packet may use that priority and send to the denoted node based on a network-wide policy. If the sender does not have that permission, it is considered infected and its traffic completely ignored (de-facto unplugged). If the ignoring mechanism is implemented properly, it can also protect against resource depletion of the classification algorithm. These checks would be especially effective against attacks from low-priority, less central nodes in a dense network graph.

It might also be interesting to investigate the ring and other network topologies and the combination and interaction of CBS with other mechanisms for TSN security, for example with Frame Replication and Elimination for path redundancy. If each node is connected to two switches, which both give access to the entire CBS-shaped network, single source attacks might have a reduced impact.

As it stands now, however, with TSN still being a newcomer to the industry and not enough data to draw sufficient conclusions about its security, future work should focus on dedicated security mechanisms to make reliable and universal guarantees.

 doi: 10.2313/NET-2025-11-3_06

# References


[1] N. Finn, "Introduction to time-sensitive networking," *IEEE Communications Standards Magazine*, pp. 22–28, jun 2018.

[2] K. Zanbouri, M. Noor-A-Rahim, J. John, C. J. Sreenan, H. V. Poor, and D. Pesch, "A comprehensive survey of wireless time-sensitive networking (tsn): Architecture, technologies, applications, and open issues," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024.

[3] J. Walrand, "A concise tutorial on traffic shaping and scheduling in time-sensitive networks," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1942–1953, 2023.

[4] Y. Seol, D. Hyeon, J. Min, M. Kim, and J. Paek, "Timely survey of time-sensitive networking: Past and future directions," *IEEE Access*, vol. 9, pp. 142 506–142 527, 2021.

[5] D. Ergenç, C. Brülhart, J. Neumann, L. Krüger, and M. Fischer, "On the security of ieee 802.1 time-sensitive networking," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.

[6] ENISA (European Union Agency for Cybersecurity), "Threat landscape." [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[7] and European Union Agency for Cybersecurity, I. Lella, M. Theocharidou, E. Magonara, A. Malatras, R. Svetozarov Naydenov, C. Ciobanu, and G. Chatzichristos, *ENISA Threat Landscape 2024 – July 2023 To June 2024*, I. Lella, M. Theocharidou, E. Magonara, A. Malatras, R. Svetozarov Naydenov, C. Ciobanu, and G. Chatzichristos, Eds., 2024.

[8] A. Mahamid, "Time sensitive networking - 802.1qci," in *Proceedings of the Seminar Innovative Internet Technologies and Mobile Communications (IITM), Winter Semester 2020/2021*, ser. Network Architectures and Services (NET), G. Carle, S. Günther, and B. Jaeger, Eds., vol. NET-2021-05-1. Munich, Germany: Chair of Network Architectures and Services, Department of Computer Science, Technical University of Munich, May 2021, pp. 9–12.

[9] R. Barton, M. Seewald, and J. Henry, "Management of ieee 802.1qci security policies for time sensitive networks (tsn)," Technical Disclosure Commons, October 2018. [Online]. Available: https://www.tdcommons.org/dpubs_series/1541

[10] F. Fischer and D. Merli, "Security considerations for ieee 802.1 time-sensitive networking in converged industrial networks," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2022, pp. 1–7.

[11] R. Sethi, A. Kadam, K. Prabhu, and N. Kota, "Security considerations to enable time-sensitive networking over 5g," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 399–407, 2022.

[12] T. Häckel, P. Meyer, F. Korf, and T. C. Schmidt, "Secure time-sensitive software-defined networking in vehicles," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 1, pp. 35–51, 2023.

[13] P. Meyer, T. Häckel, F. Korf, and T. Schmidt, "Dos protection through credit based metering – simulation based evaluation for time-sensitive networking in cars," 08 2019.

[14] S. Ramanauskaite and A. Cenys, "Taxonomy of dos attacks and their countermeasures," *Central European Journal of Computer Science*, vol. 1, no. 3, pp. 355–366, 2011.

[15] D. Karig and R. Lee, "Remote denial of service attacks and countermeasures," Princeton University Department of Electrical Engineering, Tech. Rep. CEL2001-002, 2001.

[16] A. Fadlallah and A. Serhrouchni, "Denial of service attack and schemes analysis and taxonomy," in *IEEE SETIT 2005, International Conference on Sciences of Electronic, Technology of Information and Telecommunications*, 2005, 27–31 Mar. 2005, Tunisia.

[17] M. S. Specht and R. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in *17th International Conference on Parallel and Distributed Computing Systems*, 2004, pp. 543–550.

[18] C. Douligeris and A. Mitrokotsa, "Ddos attacks and defense mechanisms: Classification and state-of-the-art," *COMPUT NETW*, vol. 44, pp. 643–666, 2004.

[19] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 39–53, 2004.

[20] M. N. J. Glenn Murray and C. Valli, "The convergence of it and ot in critical infrastructure," in *The Proceedings of 15th Australian Information Security Management Conference*, C. Valli, Ed. Edith Cowan University, dec 2017, pp. 149–155.

[21] E. Grossman, T. Mizrahi, and A. J. Hacker, "Deterministic Networking (DetNet) Security Considerations," RFC 9055, Jun. 2021. [Online]. Available: https://www.rfc-editor.org/info/rfc9055

[22] K. Stouffer, K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule *et al.*, *Guide To Operational Technology (OT) Security*. US Department of Commerce, National Institute of Standards and Technology, 2023.

[23] F. Rezabek, M. Bosk, L. Seidlitz, J. Ott, and G. Carle, "Context matters: Lessons learned from emulated and simulated tsn environments," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2024*, ser. 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2024. Institute of Electrical and Electronics Engineers Inc., 2024, pp. 499–504, publisher Copyright: © 2024 IEEE.; 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events, PerCom Workshops 2024 ; Conference date: 11-03-2024 Through 15-03-2024.

[24] *802.1Q-2022 - IEEE Standard for Local and Metropolitan Area Networks–Bridges and Bridged Networks*, IEEE Std. 802.1Q, Dec 2022. [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=10004496