



CyberShip-IoT: A Dynamic and Adaptive SDN-Based Security Policy Enforcement Framework for Ships

Sahay, Rishikesh; Meng, Weizhi; Sepúlveda Estay, Daniel Alberto; Jensen, Christian D.; Barfod, Michael Bruhn

Published in:
Future Generation Computer Systems

Link to article, DOI:
[10.1016/j.future.2019.05.049](https://doi.org/10.1016/j.future.2019.05.049)

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

[Link back to DTU Orbit](#)

Citation (APA):
Sahay, R., Meng, W., Sepúlveda Estay, D. A., Jensen, C. D., & Barfod, M. B. (2019). CyberShip-IoT: A Dynamic and Adaptive SDN-Based Security Policy Enforcement Framework for Ships. *Future Generation Computer Systems*, 100, 736-750. <https://doi.org/10.1016/j.future.2019.05.049>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Corrigendum

Corrigendum to “CyberShip-IoT: A Dynamic and Adaptive SDN-Based Security Policy Enforcement Framework for Ships” [Future Gener. Comput. Syst. 100 (2019) 736–750]

Rishikesh Sahay^a, Weizhi Meng^{a,*}, D.A. Sepulveda Estay^b, Christian D. Jensen^a, Michael Bruhn Barfod^b^a Department of Applied mathematics and Computer Science, Technical University of Denmark, DK-2800 kgs., Lyngby, Denmark^b Department of Management Engineering, Technical University of Denmark, DK-2800 kgs., Lyngby, Denmark

ARTICLE INFO

Article history:

Available online xxxx

The authors regret to inform that some small issues are found on two figures ~Figs. 8 and 9, and attach our new figures as below. The main differences are described as follows:

- (a) Experimentation is conducted for a short time (180 s)
- (b) Attack traffic is launched at 30 s.

(c) Mitigation starts at 40 s.

(d) Legitimate traffic is completely recovered at around 50 s

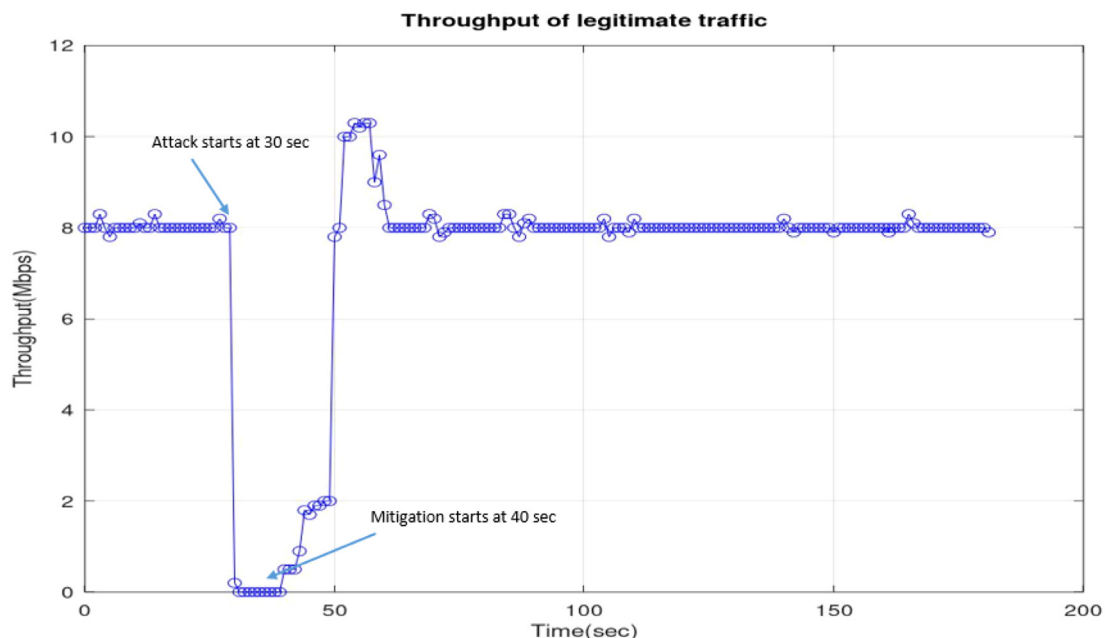


Fig. 8.

DOI of original article: <https://doi.org/10.1016/j.future.2019.05.049>.

* Corresponding author.

E-mail address: weme@dtu.dk (W. Meng).<https://doi.org/10.1016/j.future.2020.08.040>

0167-739X/© 2020 Elsevier B.V. All rights reserved.

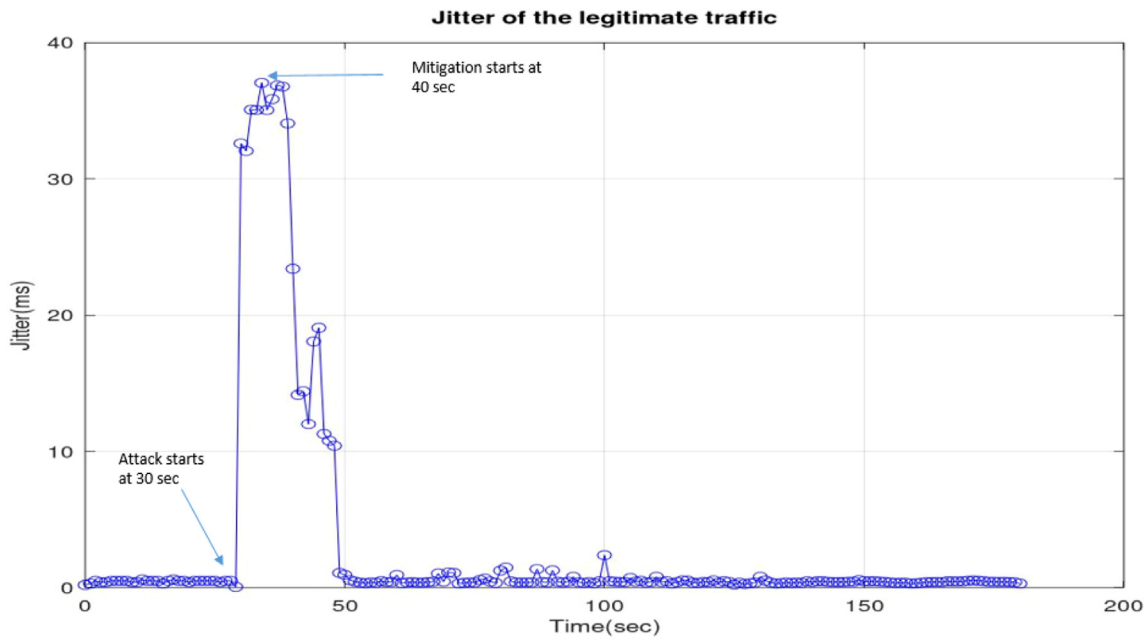


Fig. 9.

The authors would like to apologize for any inconvenience caused.