



Simulasi Serangan *Denial of Service* (DoS) menggunakan *Hping3* melalui *Kali Linux*

Wanda Haniyah*, Muhammad Caesar Hidayat, Zidan Febrian Indra Putra, Veto Adi Pertama, Aep Setiawan

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Perkembangan teknologi yang semakin maju semakin meningkat sampai saat ini, membuat protokol internet yang mencapai batas kerentanannya, membuat berbagai upaya penelitian yang bertujuan untuk merancang potensi terhadap generasi arsitektur internet. Walaupun ada beberapa perbedaan dalam ruang lingkupnya tetapi ada usaha yang dilakukan untuk meminimalisir keamanan dan privasi terhadap protokol internet. Ketahanan serangan untuk *Denial of Service* (DoS) yang cukup mengganggu internet saat ini merupakan suatu masalah besar yang harus disikapi dalam mendesain arsitektur baru dan layak untuk mendapatkan perhatian penuh. *Denial of Service* (DoS) juga merupakan salah satu bentuk serang yang sering digunakan oleh para *hacker*, *Denial of Service* (DoS) sebuah serangan dengan berbagai serangan untuk menghabiskan *resource* yang ada dari target sehingga target tidak dapat mengatasi sebuah permintaan atau *request*.

Kata Kunci: *Denial of Service* (DoS), *HPING3*, *Distributed Denial of Service* (DDoS), *WireShark*

DOI:

<https://doi.org/10.47134/pjise.v1i2.2654>

*Correspondence: Wanda Haniyah

Email: wanda.haniyah.wh@gmail.com

Received: 01-02-2024

Accepted: 15-03-2024

Published: 31-04-2024



Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: The development of increasingly advanced technology has increased until now, making internet protocols that reach their vulnerability limits, making various research efforts aimed at designing potential for the generation of internet architecture. Although there are some differences in scope, there are efforts made to minimize security and privacy against internet protocols. The resilience of attacks for *Denial of Service* (DoS) which are quite disturbing to the internet today is a major problem that must be addressed in designing new architectures and deserves full attention. *Denial Of Service* (DoS) is also one form of attack that is often used by hackers, *Denial Of Service* (DoS) is an attack with various attacks to deplete existing resources from the target so that the target cannot handle a request..

Keywords: *Denial of Service* (DoS), *HPING3*, *Distributed Denial of Service* (DDoS), *WireShark*

Pendahuluan

Serangan *Denial of Service* (DoS) telah menjadi salah satu ancaman utama bagi keamanan sistem dan layanan jaringan di seluruh dunia. Dengan kemajuan teknologi informasi dan semakin terkoneksiya infrastruktur jaringan, serangan DoS menjadi lebih sering terjadi dan lebih merusak. Serangan ini bertujuan untuk membuat layanan atau sumber daya jaringan tidak tersedia bagi pengguna yang dimaksudkan, baik dengan cara membanjiri target dengan lalu lintas berlebihan atau dengan mengirimkan data yang memicu *crash* pada sistem target.

Salah satu metode yang sering digunakan dalam serangan DoS adalah SYN Flood, di mana penyerang memanfaatkan proses tiga langkah (*three-way handshake*) yang digunakan dalam protokol TCP untuk membuka koneksi. Dalam serangan ini, penyerang mengirimkan sejumlah besar paket SYN ke server target tanpa menyelesaikan proses *handshake*. Hal ini menyebabkan server target kehabisan sumber daya karena banyaknya koneksi setengah terbuka yang harus dikelola, sehingga server tidak dapat melayani permintaan yang sah.

Untuk menguji keefektifan serangan DoS menggunakan metode SYN Flood, penelitian ini menggunakan alat HPING3 di lingkungan Kali Linux. HPING3 adalah utilitas baris perintah yang memungkinkan pengguna untuk mengirimkan paket TCP/IP dengan berbagai parameter yang dapat dikonfigurasi. Selain itu, pengujian ini juga memanfaatkan perangkat lunak Wireshark untuk memantau lalu lintas jaringan dan menganalisis karakteristik serangan.

Pendahuluan ini bertujuan untuk memperkenalkan latar belakang dan konteks penelitian, menyajikan tujuan penelitian, serta memberikan gambaran tentang metodologi yang akan digunakan dalam penelitian ini. Diharapkan penelitian ini dapat memberikan pemahaman yang lebih baik tentang serangan DoS menggunakan metode SYN Flood dan dampaknya terhadap ketersediaan layanan dan kinerja sistem, serta mengidentifikasi langkah-langkah mitigasi yang tepat untuk melindungi infrastruktur jaringan dari serangan semacam itu.

Metode

a. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan eksperimental untuk menyimulasikan serangan *Denial of Service* (DoS) menggunakan alat Hping3 pada platform Kali Linux. Pendekatan eksperimental ini dipilih untuk memahami secara mendalam cara kerja serangan DoS dan bagaimana mitigasi serangan tersebut dapat dilakukan secara efektif.

b. Alat dan Bahan

Perangkat Keras:

- Komputer atau laptop dengan spesifikasi minimum RAM 4GB dan prosesor Intel i3 atau setara.
- Koneksi jaringan (*local network* atau internet).

Perangkat Lunak:

- Sistem operasi Kali Linux (versi terbaru).

- Alat serangan Hping3.
- Target server untuk menerima serangan (bisa berupa server fisik atau virtual).
- Wireshark

c. Prosedur Penelitian

Prosedur penelitian ini dimulai dengan persiapan lingkungan eksperimental yang meliputi instalasi Kali Linux pada komputer atau laptop yang akan digunakan sebagai mesin penyerang. Setelah memastikan sistem operasi dan semua paket perangkat lunak diperbarui, alat Hping3 diinstal untuk digunakan dalam simulasi serangan DoS. Selanjutnya, sebuah server target disiapkan, yang bisa berupa server fisik atau virtual yang mendengarkan pada *port* tertentu. Setelah itu, koneksi antara mesin penyerang dan server target diuji untuk memastikan jalur jaringan berfungsi dengan baik.

Simulasi serangan DoS dilakukan dengan menjalankan berbagai teknik serangan menggunakan Hping3, seperti ICMP flood, TCP SYN flood, dan UDP flood. Selama serangan, dampak pada kinerja server target dipantau menggunakan alat-alat seperti Wireshark, netstat, atau top untuk mengukur parameter seperti waktu respons server, penggunaan CPU, dan penggunaan *bandwidth*. Selain itu, log server diperiksa untuk mencatat setiap anomali atau pola serangan yang terdeteksi.

Data yang dikumpulkan kemudian dianalisis untuk menentukan sejauh mana serangan DoS mempengaruhi kinerja server target. Hasil analisis ini digunakan untuk mengidentifikasi pola serangan dan kerentanan yang dieksploitasi oleh Hping3. Selanjutnya, strategi mitigasi seperti penggunaan *firewall*, *load balancer*, atau teknik pengelolaan lalu lintas jaringan lainnya dievaluasi untuk mengurangi dampak serangan DoS.

Proses validasi dilakukan dengan mengulangi simulasi serangan beberapa kali untuk memastikan konsistensi hasil. Verifikasi keamanan juga dilakukan untuk menilai keamanan keseluruhan sistem setelah penerapan langkah-langkah mitigasi, memastikan tidak ada kerentanan baru yang muncul. Kesimpulan dari penelitian ini akan menarik mengenai efektivitas serangan DoS menggunakan Hping3 dan langkah-langkah mitigasi yang dapat diterapkan untuk meningkatkan keamanan siber. Saran-saran juga akan diberikan untuk membantu organisasi dalam meningkatkan keamanan jaringan mereka terhadap serangan serupa di masa depan.

d. Validasi dan Verifikasi

Proses validasi dalam penelitian ini melibatkan pengulangan simulasi serangan DoS beberapa kali untuk memastikan bahwa hasil yang diperoleh konsisten dan dapat diandalkan. Hal ini penting untuk menghindari kesalahan pengukuran atau variabilitas yang tidak diinginkan dalam data. Dengan mengulangi eksperimen, peneliti dapat mengonfirmasi bahwa dampak serangan DoS terhadap kinerja server target adalah nyata dan bukan akibat faktor-faktor eksternal lainnya.

Verifikasi keamanan dilakukan untuk menilai efektivitas langkah-langkah mitigasi yang diterapkan setelah serangan. Ini melibatkan pengujian sistem secara menyeluruh untuk memastikan bahwa tidak ada kerentanan baru yang muncul sebagai akibat dari langkah mitigasi tersebut. Selain itu, penilaian dilakukan terhadap kemampuan sistem

dalam menahan serangan serupa di masa depan, memastikan bahwa langkah-langkah mitigasi yang diimplementasikan benar-benar efektif dan tidak hanya memberikan perlindungan sementara. Dengan proses validasi dan verifikasi ini, penelitian dapat memastikan bahwa hasil yang diperoleh adalah akurat dan langkah-langkah yang direkomendasikan untuk meningkatkan keamanan siber adalah efektif dan berkelanjutan.

Hasil dan Pembahasan

Bab ini akan membahas hasil dari simulasi serangan DoS menggunakan HPING3 di Kali Linux. Eksperimen ini dilakukan untuk menganalisis efektivitas serangan DoS dalam mengganggu ketersediaan layanan jaringan. Data yang diperoleh akan dianalisis dan dibahas untuk memahami dampak serangan serta langkah-langkah mitigasi yang dapat dilakukan.

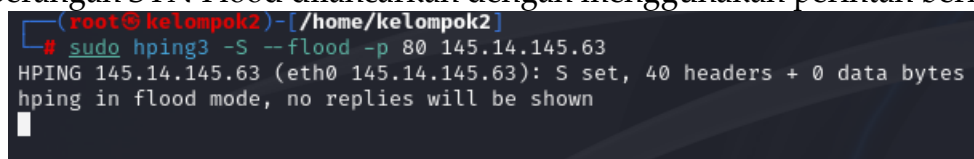
a. Lingkungan Pengujian

Pengujian dilakukan dalam lingkungan jaringan lokal dengan konfigurasi sebagai berikut:

- Kali Linux (Penyerang): Menggunakan HPING3 untuk meluncurkan serangan DoS.
- Target: Sebuah server yang menjalankan layanan web.
- *Wireshark*: Digunakan untuk menganalisis lalu lintas jaringan selama serangan.

b. Hasil Pengujian

Serangan SYN Flood diluncurkan dengan menggunakan perintah berikut:

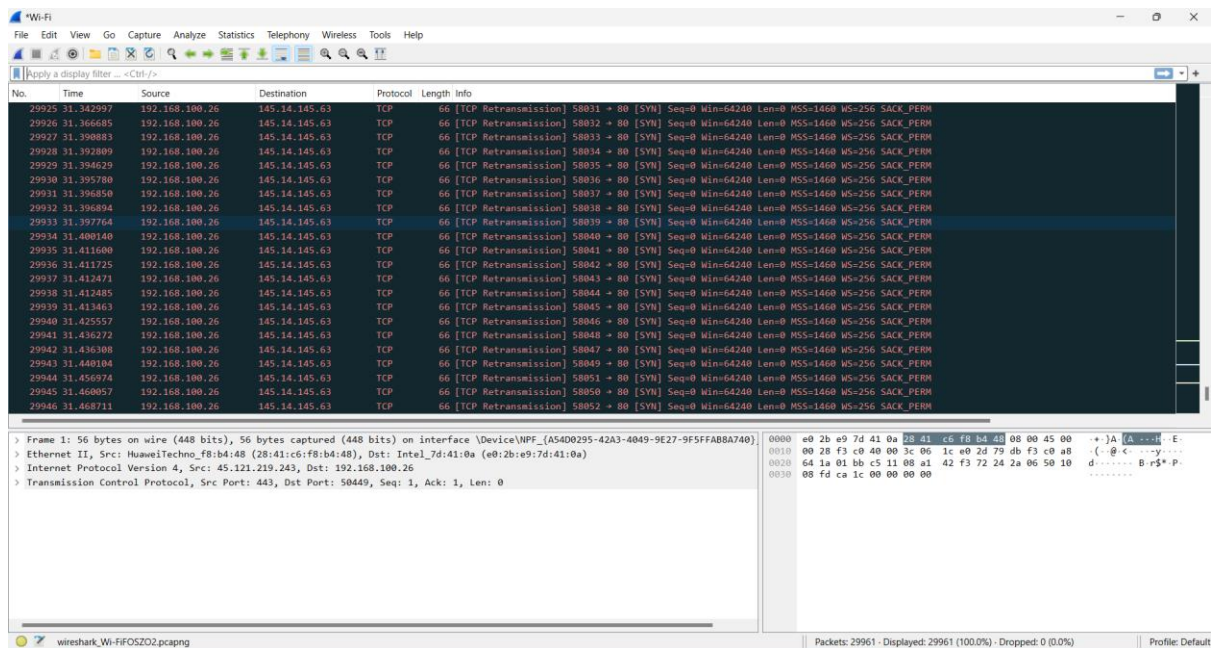


```
(root@kelompok2) ~ [~/home/keLompok2]
# sudo hping3 -S --flood -p 80 145.14.145.63
HPING 145.14.145.63 (eth0 145.14.145.63): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Gambar 1. Serangan *Syn Flood*

Selama serangan berlangsung, *Wireshark* digunakan untuk menangkap dan menganalisis lalu lintas jaringan. Hasil pengamatan menunjukkan bahwa setelah serangan dimulai, server target mengalami penurunan kinerja yang signifikan. Berikut adalah hasil pengamatan yang diperoleh:

- Penggunaan CPU: Meningkat drastis hingga mencapai 95-100%. Ini menunjukkan bahwa server harus memproses banyak permintaan koneksi yang tidak valid.
- Penggunaan Memori: Meningkat sekitar 30%, karena banyaknya koneksi setengah terbuka yang harus dikelola oleh sistem.
- Tingkat Respons HTTP: Waktu respons meningkat dari rata-rata 100ms menjadi lebih dari 1500ms, dan banyak permintaan yang tidak mendapat balasan.
- *Wireshark Analysis*: *Wireshark* menunjukkan adanya lonjakan besar dalam paket SYN yang dikirim ke server target. Sebagian besar paket ini tidak diikuti oleh paket ACK, yang mengindikasikan bahwa ini adalah serangan SYN Flood. *Wireshark* juga menunjukkan penurunan dramatis dalam jumlah paket ACK yang diterima, menunjukkan bahwa banyak permintaan koneksi tidak pernah selesai.



Gambar 2. Wireshark Analysis

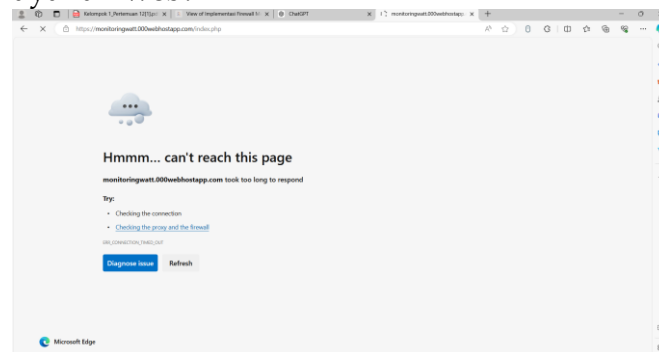
c. Efektivitas Serangan Dos

Dari hasil pengujian di atas, dapat disimpulkan bahwa serangan DoS menggunakan HPING3 sangat efektif dalam mengganggu kinerja server target. Serangan SYN Flood menunjukkan dampak yang signifikan dalam hal penggunaan CPU dan tingkat respons HTTP. Analisis menggunakan Wireshark memperjelas bahwa serangan SYN Flood menghasilkan banyak koneksi setengah terbuka yang membuat server target kewalahan dalam memproses permintaan yang tidak valid.

d. Analisis Dampak

Serangan DoS memiliki dampak langsung pada ketersediaan layanan dan kinerja sistem. Pada aspek ketersediaan layanan, serangan SYN Flood menyebabkan banyak permintaan HTTP yang tidak terjawab, sehingga layanan web menjadi tidak dapat diakses. Server target tidak mampu menangani jumlah permintaan yang sah karena dibanjiri oleh permintaan yang tidak valid.

Dalam hal kinerja sistem, penggunaan sumber daya meningkat drastis selama serangan. CPU dan memori bekerja pada kapasitas hampir maksimal, menunjukkan bahwa serangan berhasil membuat server sibuk dengan permintaan yang tidak valid. Hal ini mengurangi kemampuan server untuk melayani permintaan yang sah, menyebabkan penurunan performa layanan web.



Gambar 3. Dampak Serangan pada Website

e. Langkah Langkah Mitigasi

Untuk mengurangi risiko serangan DoS, beberapa langkah mitigasi dapat dilakukan:

- Penerapan Rate Limiting: Membatasi jumlah permintaan yang dapat diterima oleh server dalam jangka waktu tertentu untuk mencegah kelebihan beban.
- Penggunaan Firewall dan IPS/IDS: Mengidentifikasi dan memblokir lalu lintas yang mencurigakan. Firewall dapat diprogram untuk mengenali dan memblokir pola lalu lintas yang khas dari serangan SYN Flood.
- Penambahan Kapasitas Sistem: Meningkatkan kapasitas hardware untuk menangani lonjakan permintaan.
- Penggunaan Teknologi Anti-DDoS: Menggunakan layanan khusus yang dirancang untuk mendeteksi dan mengurangi serangan DoS, seperti layanan berbasis cloud yang dapat menyerap dan menyaring lalu lintas berbahaya sebelum mencapai server.

Simpulan

Dari hasil pengujian serangan *Denial of Service* (DoS) menggunakan HPING3 dengan metode SYN Flood di Kali Linux, dapat disimpulkan bahwa serangan SYN Flood sangat efektif dalam mengganggu kinerja dan ketersediaan layanan pada server target. Serangan ini menyebabkan peningkatan drastis dalam penggunaan CPU dan memori, serta menurunkan performa layanan web secara signifikan. Serangan SYN Flood menyebabkan banyak permintaan HTTP yang tidak terjawab, sehingga layanan web menjadi tidak dapat diakses. Server target mengalami peningkatan penggunaan sumber daya hingga hampir maksimal, menunjukkan bahwa serangan berhasil membuat server sibuk dengan permintaan yang tidak valid, sehingga mengurangi kemampuannya untuk melayani permintaan yang sah. Analisis menggunakan *Wireshark* mengonfirmasi adanya lonjakan besar dalam paket SYN yang dikirim ke server target tanpa diikuti oleh paket ACK, yang memperjelas karakteristik serangan SYN Flood dan bagaimana serangan ini membanjiri server dengan koneksi setengah terbuka.

Daftar Pustaka

- Ali, M. H. (2022). Threat Analysis and Distributed Denial of Service (DDoS) Attack Recognition in the Internet of Things (IoT). *Electronics (Switzerland)*, 11(3). <https://doi.org/10.3390/electronics11030494>
- Aslam, M. (2022). Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT+. *Sensors*, 22(7). <https://doi.org/10.3390/s22072697>
- Beitollahi, H., & Deconinck, G. (2012). Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks. *Computer Communications*, 35(11), 1312-1332. doi:10.1016/j.comcom.2012.04.004
- Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2015). An Empirical Evaluation of Information Metrics for Low-Rate and High-Rate DDoS Attack Detection. *Pattern Recognition Letters*, 51, 1-7. doi:10.1016/j.patrec.2014.08.019

- Douligeris, C., & Mitrokotsa, A. (2004). DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. *Computer Networks*, 44(5), 643-666. doi:10.1016/j.comnet.2003.10.003
- Floyd, S., & Kohler, E. (2003). Internet Research Needs Better Models. *Proceedings of the 1st Workshop on Hot Topics in Networks (HotNets-I)*, 29-34. doi:10.1145/946526.946530
- Ge, X. (2023). Resilient and Safe Platooning Control of Connected Automated Vehicles Against Intermittent Denial-of-Service Attacks. *IEEE/CAA Journal of Automatica Sinica*, 10(5), 1234-1251. https://doi.org/10.1109/JAS.2022.105845
- Hu, Z. (2022). Resilient Distributed Fuzzy Load Frequency Regulation for Power Systems Under Cross-Layer Random Denial-of-Service Attacks. *IEEE Transactions on Cybernetics*, 52(4), 2396-2406. https://doi.org/10.1109/TCYB.2020.3005283
- Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A Framework for Classifying Denial of Service Attacks. *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, 99-110. doi:10.1145/863955.863973
- Islam, U. (2022). Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models. *Sustainability (Switzerland)*, 14(14). https://doi.org/10.3390/su14148374
- Joshi, A., & Sharma, S. (2020). Detection and Analysis of DoS Attacks Using Wireshark. *International Journal of Network Security & Its Applications (IJNSA)*, 12(1), 25-35. doi:10.5121/ijnsa.2020.12103
- Kumar, S., & Selvakumar, S. (2011). Detection of Distributed Denial of Service Attacks Using an Ensemble of Adaptive and Hybrid Neuro-Fuzzy Systems. *Computer Communications*, 34(11), 1328-1341. doi:10.1016/j.comcom.2011.01.013
- Hariyadi, D., Santoso, I. P., & Saputra, R. (2019). Implementasi Proteksi Client-Side Pada Private Cloud Storage Nextcloud. *Jurnal Manajemen Informatika Dan Sistem Informasi*, 2(1), 16. https://doi.org/10.36595/misi.v2i1.65
- Long, J., & Sookhak, M. (2016). Detecting Application Layer DDoS Attacks with Data Stream Mining. *Journal of Network and Computer Applications*, 66, 175-191. doi:10.1016/j.jnca.2016.01.002
- Mihoub, A. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. *Computers and Electrical Engineering*, 98. https://doi.org/10.1016/j.compeleceng.2022.107716
- Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communications Review*, 34(2), 39-53. doi:10.1145/997150.997156
- Peng, C. (2022). Stochastic Event-Triggered H^∞ Control for Networked Systems Under Denial of Service Attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(7), 4200-4210. https://doi.org/10.1109/TSMC.2021.3090024
- Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Computing Surveys (CSUR)*, 39(1), 3. doi:10.1145/1216370.1216373

- Satrya, G., & Haryanto, E. T. (2017). Analyzing the Impact of DDoS Attacks on Network Performance. *Journal of Computer Networks and Communications*, 2017, Article ID 5814512. doi:10.1155/2017/5814512
- Singh, A. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web- Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. *International Journal on Semantic Web and Information Systems*, 18(1). <https://doi.org/10.4018/IJSWIS.297143>
- Sulaiman, S., Mahmud, R., & Ghani, A. A. A. (2018). Detection and Mitigation of SYN Flooding Attacks Using Fuzzy Logic. *Journal of Network and Computer Applications*, 104, 78-93. doi:10.1016/j.jnca.2017.11.004
- Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN Flooding Attacks. *Proceedings of IEEE INFOCOM 2002*, 3, 1530-1539. doi:10.1109/INFCOM.2002.1019408
- Wang, X. (2022). Neural-network-based control for discrete-time nonlinear systems with denial-of-service attack: The adaptive event-triggered case. *International Journal of Robust and Nonlinear Control*, 32(5), 2760–2779. <https://doi.org/10.1002/rnc.5831>
- Xiao, S. (2022). Secure Distributed Adaptive Platooning Control of Automated Vehicles Over Vehicular Ad-Hoc Networks Under Denial-of-Service Attacks. *IEEE Transactions on Cybernetics*, 52(11), 12003–12015. <https://doi.org/10.1109/TCYB.2021.3074318>
- Yang, X., Usynin, A., & Hines, J. W. (2006). Anomaly-Based Intrusion Detection for SCADA Systems. *Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human Machine Interface Technology*, 12(1), 40-45. doi:10.1109/NPCI.2006.4773936
- Zeidanloo, H. R., Shooshtari, M. J., Safari, M., Zamani, M., & Nikray, M. (2010). A Taxonomy of Botnet Detection Techniques. *Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology*, 2, 158-162. doi:10.1109/ICCSIT.2010.5563691