DETEKSI SERANGAN *MAN IN THE MIDDLE* PADA IoT INDUSTRI (IIoT) SCADA MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Linda Purnama
09011381621085

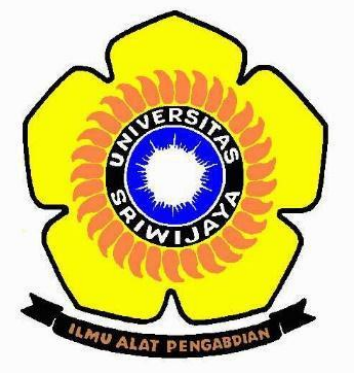
JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2021

DETEKSI SERANGAN *MAN IN THE MIDDLE* PADA IoT INDUSTRI (IIoT) SCADA MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer



Oleh :

Linda Purnama
09011381621085

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021

LEMBAR PENGESAHAN

DETEKSI SERANGAN *MAN IN THE MIDDLE* PADA IoT INDUSTRI (IIoT) SCADA MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

LINDA PURNAMA
0901138121085

Palembang, Juli 2021

Pembimbing I,

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Pembimbing II,

Ahmad Heryanto, S.Kom., M.T.
NIP. 198701222015041002

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Jum'at

Tanggal : 9 Juli 2021

Tim Penguji :

1. **Ketua** : **Ahmad Fali Oklilas, M.T.**
2. **Sekretaris** : **Tri Wanda Septian, M.SC.**
3. **Penguji** : **Huda Ubaya, S.T., M.T.**

Mengetahui 21/8/21
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Linda Purnama

NIM : 09011381621085

Judul : Deteksi Serangan *Man In The Middle* Pada IoT Industri (IIoT) SCADA Menggunakan Metode *Support Vector Machine*

Hasil Pengecekan *Software iThenticate/Turnitin* : 13%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang belaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dalam paksaan.

Palembang, Juli 2021

Yang menyatakan,

Linda Purnama

NIM. 09011381621085

KATA PENGANTAR

Puji dan syukur kepada Allah SWT, atas segala karunia dan rahmat-Nya yang telah memberikan penulis kesehatan dan kesempatan sebaik-baiknya, sehingga penulis dapat menyelesaikan Proposal Tugas Akhir ini dengan judul "Deteksi Serangan *Man In The Middle* pada IoT industri (IIoT) SCADA Menggunakan Metode *Support Vector Machine*"**.**

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu baik dari segi moril ataupun materil serta memberikan kemudahan, dorongan, saran dan kritik selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga penulisan proposal tugas akhir ini dapat berjalan dengan lancar.
2. Kedua Orangtua serta keluarga yang selalu memberikan semangat dan do'a.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Ibu Prof. Dr. Ir. Siti Nurmaini, M.T., selaku Dosen Pembimbing Akademik di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Bapak Ahmad Heryanto, S.Kom,. M.T. selaku Dosen Pembimbing II Tugas Akhir di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Mbak Renny Virgasari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
9. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Sahabatku Nur Halimah Nasution, Sisilia Chandra, Bagas Syaputra, Pipo Inzaghi, Erik Yosvian dan M. Redho Fauzan.
11. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
12. Almamaterku.

Akhir kata penulis menyadari bahwa dalam penulisan Proposal Tugas Akhir ini masih banyak terdapat kekurangan dan kesalahan. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun agar lebih baik lagi dimasa akan datang dan semoga bermanfaat bagi kita semua baik dalam dunia Pendidikan maupun dalam lingkungan masyarakat.

Palembang, Juli 2021
Penulis

Linda Purnama
Nim. 09011381621085

Detection Of Man In The Middle Attack On Industrial IoT (IIoT) SCADA Using Support Vector Machine Method

Linda Purnama (09011381621085)

Department of Computer Systems, Faculty of Computer Science

Sriwijaya University

E-mail : *lindapurnama1908@gmail.com*

Abstract

Supervisory Control And Acquisition (SCADA) system is an automated industrial control system used to control and monitor various stages of a widespread industry, where data acquisition is very important in the operation of the system. One of the communication protocols used in SCADA communication is IEC 60870-5-104. The IEC 60870-5-104 protocol has vulnerabilities security in application layer and data link layer. Man In The Middle attack has a big enough risk in SCADA system, where attacker secretly cut off communication between two or more devices. In this research, it is classified using the Support Vector Machine (SVM) to distinguish normal and attack packages. From the result of the SVM algorithm with confusion matrix, the TPR value is 100%, the FPR value of around 0.045%, the TNR value of around 97.82%, the FNR value is 0%, the precision value of around 99.85%, the F-1 Score ranged 99.92%, while the value of accuracy is 99.86%.

Keywords : *Supervisory Control And Acquisition* (SCADA), *Man In The Middle, Intrusion Detection System, Support Vector Machine, Confusion Matrix*

Deteksi Serangan *Man In The Middle* Pada IoT Industri (IIoT) SCADA Menggunakan Metode *Support Vector Machine*

Linda Purnama (09011381621085)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Univesitas Sriwijaya
E-mail : lindapurnama1908@gmail.com

Abstrak

Sistem *Supervisory Control And Acquisition* (SCADA) adalah sistem kontrol industri otomatis yang digunakan untuk mengontrol serta memantau berbagai tahapan industri yang menyebar luas, dimana akuisisi data sangatlah penting didalam pengoperasian sistem. Salah satu protokol komunikasi yang digunakan dalam komunikasi SCADA adalah IEC 60870-5-104. Protokol IEC 60870-5-104 memiliki kerentanan pada keamanan *application layer* dan *data link layer*. Serangan *Man In The Middle* memiliki resiko cukup besar didalam sistem SCADA, dimana penyerang secara diam-diam memotong komunikasi antara dua perangkat atau lebih. Pada penelitian ini diklasifikasi menggunakan *Support Vector Machine* (SVM) untuk membedakan paket normal dan serangan. Dari hasil algoritma SVM dengan *confusion matrix* diperoleh nilai TPR adalah 100%, nilai FPR yang berkisar rentang 0.045%, nilai TNR berkisar pada 97.82%, nilai FNR adalah 0%, nilai Presisi berkisar pada 99.85%, nilai F-1 Score berkisar pada 99.92%, sedangkan nilai akurasi adalah 99.86%.

Kata Kunci : *Supervisory Control And Acquisition* (SCADA), *Man In The Middle*, *Intrusion Detection System*, *Support Vector Machine*, *Confusion Matrix*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Sistem *Supervisory Control And Data Acquisition* (SCADA) ialah sistem kontrol industri otomatis yang digunakan untuk mengontrol serta memantau berbagai tahapan industri misalnya penyaluran minyak dan gas, penyaluran air serta jaringan tenaga listrik yang menyebar luas, dimana akuisisi data sangatlah penting didalam pengoperasian sistem. Secara historis, sistem SCADA ini memiliki jaringan pribadi dan khusus. Tetapi, dikarenakan luasnya penyebaran perangkat SCADA, sekarang komunikasi sistem SCADA menggunakan internet [1], dimana menyebabkan pengungkapan sistem SCADA ke dunia maya serta membuatnya kerentanan akan attacker dunia maya.

Dilain sisi, serangan *Man In The Middle* memiliki resiko cukup besar didalam sistem SCADA [2]. Serangan M*an In The Middle* merupakan jenis serangan dimana penyerang secara diam-diam memotong komunikasi antara dua perangkat atau lebih, dimana ia mampu mencegat, memodifikasi, mengubah ataupun mengganti lalu lintas komunikasi perangkat korban [3].

Salah satu protokol komunikasi SCADA adalah IEC 60870-5-104 digunakan untuk mengirim pesan telekontrol dasar antara dua sistem melalui jaringan TCP/IP standar, yang memungkinkan transmisi data secara bersamaan antar sejumlah layanan serta perangkat [4]. Protokol tersebut mempunyai kerentanan terhadap keamanan a*pplication layer* berupa serangan *spoofing* dan serangan *non-repudiation*, sementara kerentanan keamanan di d*ata link layer* berupa serangan *modification data*, *snipping* serta *replay attack* [5].

Intrusion Detection System (IDS) adalah sistem yang memantau suatu lalu lintas jaringan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan. Penggunaan IDS di jaringan SCADA merupakan rancangan yang cenderung baru. Sejumlah studi mempergunakan metode IDS yang sudah dijalankan di sistem SCADA, misalnya signature-based serta anomaly-based [6]–[8]. Proyek Digital Bond Quickdraw [6] membuat IDS berbasis signature untuk Modbus, s7, DNP3 dan bacnet menggunakan snort.

Dalam penelitian [7] membahas mengenai sistem deteksi anomali berbasis *model-based* untuk mengenali serangan ke gardu induk tenaga listrik berdasarkan protokol IEC 60870-5-104, menggunakan tiga model serangan yang berbeda diantaranya, *DoS, Arp Spoofing* dan C*ommand Injection.* Model deteksi dirancang dengan beberapa algoritma *Supervised Learning* misalnya *Naive Bayes, Nearest Neighbor, Decision Tree* serta *Rule Learners,* dari hasil pengujian yang diperoleh bahwasannya algoritma *Rule Learners* mempunyai akurasi terbaik yakni 91,69%. Sementara di penelitian lainnya [8] memperlihatkan hasil pendeteksian anomali menggunakan algoritma *Support Vector Machine* mempunyai akurasi yang lebih baik.

Support Vector Machine (SVM) ialah metode data mining yang mempunyai akurasi yang lebih baik saat mengklasifikasikan pola paket data lalu lintas jaringan [9]. SVM juga mampu memisahkan antara data serangan dan data normal dengan cara pembagian antar *class*.

Dari sejumlah ulasan tersebut, penelitian berikut akan merancang *Intrusion Detection System* berbasis *anomaly* untuk deteksi serangan *Man In The Middle* pada IoT Industri (IIoT) SCADA protokol IEC 60870-5-104 dengan menggunakan penerapan metode algoritma *Support Vector Machine.*

1.2. Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Melakukan pengenalan pola serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA.
2. Membedakan antara paket normal dan paket serangan pada IoT Industri (IIoT) SCADA sehingga dapat mendeteksi serangan *Man In The Middle Arp Spoofing.*
3. Menerapkan algoritma *Support Vector Machine* untuk deteksi paket serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA.
4. Menghitung akurasi deteksi serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA menggunakan metode *Support Vector Machine.*

1.3. Manfaat

Adapun manfaat dari penelitian Tugas Akhir ini adalah sebagai berikut :

1. Dapat memberikan kemudahan dalam mengenali pola serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA.
2. Dapat membedakan paket normal dan paket serangan pada IoT Industri (IIoT) SCADA.
3. Dapat mendeteksi serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA.
4. Dapat mengetahui tingkat akurasi algoritma *Support Vector Machine* dalam deteksi serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA.

1.4. Rumusan Masalah

Adapun rumusan masalah dalam penelitian Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana membedakan paket data normal dengan paket data serangan *Man In The Middle Arp Spoofing* ?
2. Bagaimana algoritma *Support Vector Machine* ini dapat mengenali serangan *Man In The Middle Arp Spoofing* pada IoT Industri (IIoT) SCADA menggunakan paket data normal ?

1.5. Batasan Masalah

Batasan masalah dalam penelitian Tugas Akhir ini adalah sebagai berikut :

1. Penelitian dilakukan pada IoT Industri (IIoT) SCADA protokol IEC 60870-5-104.
2. Serangan yang dideteksi hanya serangan *Man In The Middle Arp Spoofing.*
3. Mengklasifikasi serangan *Man In The Middle Arp Spoofing* menggunakan *Support Vector Machine* kernel *linear.*
4. Pengujian dilakukan secara *offline.*
5. Menggunakan dataset yang tercapture paket normal dan paket serangan *Man In The Middle Arp Spoofing.*

6. Tidak membahas cara pencegahan serangan *Man In The Middle.*

1.6. Metodologi Penelitian

Metodologi yang digunakan pada penelitian tugas akhir ini adalah sebagai berikut :

1. Studi Pustaka

   Dalam tahapan berikut penulis mengulas dan mempelajari sumber-sumber referensi dari media pembelajaran seperti buku, naskah ilmiah serta artikel yang terkait langsung pada penelitian Tugas Akhir ini.

2. Perancangan Sistem

   Tahapan ini merupakan tahapan untuk menetukan perangkat keras maupun perangkat lunak yang cocok untuk merancang dan membangun sistem deteksi serangan *Man In The Middle Arp Spoofing* menggunakan algoritma SVM.

3. Klasifikasi

   Dalam tahapan berikut penulis melakukan proses pengklasifikasikan data normal dan serangan *Man In The Middle Arp Spoofing* dengan menggunakan algoritma SVM.

4. Hasil dan Analisis

   Tahapan berikut berupa hasil klasifikasi pada penelitian tersebut kemudian dianalisis hasil tersebut dengan tujuan untuk dapat melihat tingkat performa dari penelitian Tugas Akhir ini.

5. Kesimpulan dan Saran

   Dalam tahapan berikut merupakan langkah akhir, hasil dari semua langkah yang dilakukan sebelumnya akan dirumuskan menjadi suatu kesimpulan.

1.7. Sistematika Penulisan

Dalam penyusunan tugas akhir ini dibuat sistematika penulisan untuk memudahkan dan memperjelas isi dari setiap bab sebagai berikut :

BAB I. PENDAHULUAN

Bab ini berupa penjelasan mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, Metodologi Penelitian dan Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisi mengenai dasar teori dari penelitian yaitu *Supervisory Control And Data Acquisition, Industrial Internet Of Things (IIoT), Man In The Middle, Intrusion Detection System, Support Vector Machine* dan yang berhubungan dengan penelitian tugas akhir.

BAB III. METODOLOGI PENELITIAN

Bab ini berupa penjelasan secara sistematis, mengenai bagaimana proses penelitian dilakukan, tahapan perancangan sistem dan penerapan metode dalam penelitian ini.

BAB IV. HASIL DAN ANALISA

Bab ini berupa penjelasan dari hasil yang didapatkan dari pengujian serta dilakukan analisis terhadap perancangan sistem dan penerapan metode dalam penelitian ini.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan yang didapatkan dari hasil penelitian, serta menjawab tujuan yang hendak dicapai seperti yang tertera pada BAB I (Pendahuluan), dan memberikan saran untuk pengembangan penelitian selanjutnya.

\

DAFTAR PUSTAKA

[1] M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, and M. Samaka, "SCADA System Testbed for Cybersecurity Research Using Machine Learning Approach," *Futur. Internet,* vol. 10, Aug. 2018.

[2] P. Radoglou-grammatikis, P. Sarigiannidis, and I. Giannoulakis, "Attacking IEC-60870-5-104 SCADA Systems," *1st IEEE Serv. Work Secur. Resil.Internet Things,* pp.41-46, 2019.

[3] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man In The Middle Attacks," *1st IEEE Commun. Surv.Tutorials,* vol. 18, no. 3, pp. 2027–2051, 2016.

[4] Q. S. Qassim, N. Jamil, M. Daud, N. Ja, and S. Yussof, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *Int J. Eng. Technol*., vol. 7, pp. 153–159, 2018.

[5] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA communication protocols : vulnerabilities , attacks and possible mitigations," *CSI Trans. ICT,* vol. 1, no. 2, pp. 135–141, 2013.

[6] "GitHub - digitalbond/Quickdraw-Snort: Digital Bond's IDS/IPS rules for ICS and ICS protocols." [Online]. Available: https://github.com/digitalbond/Quickdraw-Snort. [Accessed: 02-Nov-2020]

[7] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," *ARES '17*, pp. 1-7, 2017.

[8] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2019.

[9] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access,* vol. 6, pp. 33789–33795, 2018.

[10] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016.

[11] M. Petr, “Description and analysis of IEC 104 Protocol,” pp. 38, 2017.

[12] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, “Intrusion Detection System for IEC 60870-5-104 based SCADA networks,” *IEEE Power Energy Soc. Gen. Meet.*, 2013.

[13] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (IIoT): An analysis framework,” *Comput. Ind.*, vol. 101, pp. 1–12, 2018.

[14] G. Falco, C. Caldera, and H. Shrobe, “IIoT Cybersecurity Risk Modeling for SCADA Systems,” *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4486–4495, 2018.

[15] S. Rachel, “An Overview of the Man-In-The-Middle Attack,” *Natl. Conf. Contemp. Res.Innov. Comput.Sci.*, pp. 1–6, 2017.

[16] O. Eigner, P. Kreimel, and P. Tavolato, “Detection of Man-in-the-Middle Attacks on Industrial Control Networks,” in *International Conference on Software Security and Assurance (ICSSA)*, 2016, pp. 64–69.

[17] J J. Jabez and B. Muthukumar, “Intrusion detection system (ids): Anomaly detection using outlier detection approach,” *Procedia Comput. Sci.*, vol. 48, pp. 338–346, 2015.

[18] J. Peng, K. K. R. Choo, and H. Ashman, “User profiling in intrusion detection: A review,” *J. Netw. Comput. Appl.*, vol. 72, pp. 14–27, 2016.

[19] U. Albalawi, “A comprehensive analysis on intrusion detection in iot based smart environments using machine learning approaches,” *Int. J. Sci. Technol. Res.*, vol. 9, no. 4, pp. 1646–1652, 2020.

[20] S. Akbar, D. K. N. Rao, and D. J. A. Chandulal, “Intrusion Detection System Methodologies Based on Data Analysis,” *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010.

[21] N. J. Khan and Javed Akhtar, “A Survey on Intrusion Detection Systems and Classification Techniques,” *IJSRSET, India*, vol. 2, no. 5, pp. 202–208, 2016.

[22] Z. Rustam and N. P. A. A. Ariantari, “Comparison between support vector machine and fuzzy Kernel C-Means as classifiers for intrusion detection system using chi-square feature selection,” *AIP Conf. Proc.*, vol. 2023, 2018.

[23] P. Maynard, K. McLaughlin, and S. Sezer, “An Open Framework for Deploying Experimental SCADA Testbed Networks,” *Ind. Control Syst. Cyber Secur.*, pp. 89–98,Aug. 2018.

[24] G. K. Armah, G. Luo, and K. Qin, “A Deep Analysis of the Precision Formula for Imbalanced Class Distribution,” *Int. J. Mach. Learn. Comput.*, vol. 4, no. 5, pp. 417–422, 2014.

[25] S. Andrews, I. Tsochantaridis, and T. Hofmann, “Support Vector Machines for Multi ple-Instance Learning,” *Adv. Neural Inf. Process.Syst*.(NIPS'02), vol.53, no. 9, pp. 1689-1699, 2002.