REVIEW PERKEMBANGAN TEKNIK STEGANOGRAFI DALAM LAPISAN JARINGAN KOMPUTER

Eka Ardhianto[1], W.T. Handoko[2], Edi Supriyanto[3],
[1,2]Program Studi Teknik Informatika, Universitas Stikubank
[3]Program Studi Sistem Informasi, Universitas Stikubank
Email : [1]eka@unisbank.ac.id, [2]wthandoko@edu.unisbank.ac.id,
[3]edy_supriyanto@edu.unisbank.ac.id

Abstrak

Proses kriptografi masih sering dikombinasikan dengan steganografi dalam mekanisme pengamanan data dan penyembunyian data. Pengamanan data ini tidak hanya dilakukan pada data yang bersifat berhenti dan tersimpan pada komputer. Perkembangan teknologi komunikasi dalam jaringan memberikan revolusi dalam mengamankan data berjalan melalui saluran transmisi. Dalam paper ini dilakukan sebuah systematicliteraturereview (SLR) yang membahas perkembangan teknik steganografi data berjalan serta memberikan gambaran pengembangan penelitian untuk meningkatkan kekuatan proses pengamanan data.

Katakunci : data security, steganography, network layer, transport layer

1. PENDAHULUAN

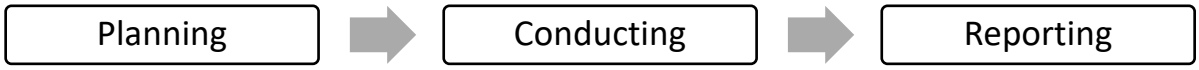
Keamanan informasi hingga saat ini masih terus masih digunakan dalam berbagai bidang, misalnya keamanan dalam berkomunikasi dan transaksi melalui sebuah perantara jaringan. Dalam melakukan pengamanan data teknik kriptografi sudah dapat memberikan keamanan dengan melakukan proses enkripsi dan dekripsi [1] . Meskipun demikian serangan terhadap sebuah ciphertext masih dapat terjadi. Hal ini karena dalam kriptografi produk yang dihasilkan masih memperlihatkan kecurigaan terhadap pesan yang dirahasiakan. Steganography hadir dengan menyembunyikan pesan kedalam sebuah cover. keuntungan dari steganografi adalah bahwa orang yang tidak berhak tidak akan menduga keberadaan sebuah pesan[1].

Peranan internet dan jaringan komunikasi saat ini sudah mengakomodasi dalam pertukaran sebuah data dan informasi. Hal ini sangat menguntungkan dalam percepatan pengiriman sebuah pesan. Namun perlu difikirkan bahwa kerahasiaan sebuah data dan informasi adalah menjadi sesuatu yang perlu diperhatikan. Mekanisme steganografi dapat memberikan kekuatan dalam penyembunyian data melalui sebuah cover[2]. Tahun 2003, sebuah penelitian melakukan penggabungan steganography dengan teknologi jaringan yang disebut dengan Network Steganography[3]. Hal ini akan mengakibatkan penyembunyian data menjadi lebih kuat dan lebih sulit di deteksi. Pokok dari networksteganography adalah memanfaatkan 7 protokol dalam Open System Interconnection (OSI) sebagai cover dari data[3].

Dalam paper ini akan menyuguhkan penelusuran perkembangan teknik steganografidata berjalan yang melakukan modifikasi dalam lapisan OSI dan pembahasan mengenai kegiatan penelitian yang telah dilakukan dengan sistematicliteraturereview (SLR).

2. METODE

Dalam melakukan systematic literature review, dilakukan beberapa fase pekerjaan yang dapat gambarkan pada gambar 1.



Gambar 1. Tahapan SLR

3. PERANCANGAN

Fase ini adalah tahapan awal dalam pelaksanaan SLR. Pada fase ini dilakukan penentuan topik dan Riset Question yang akan digunakan sebagai penuntun proses pencarian literatur. Sebagai topik diambil adalah steganographysocketprogramming. Dan QR yang digunakan adalah sebagai berikut :

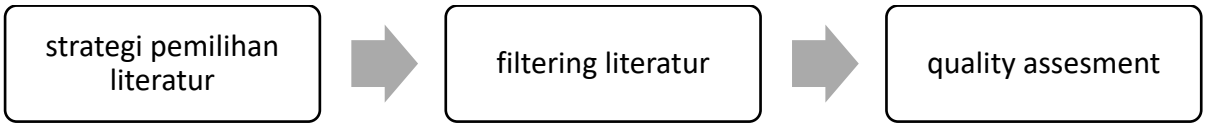
QR1 : apakah terdapat kegiatan penelitian tentang stegaografi dalam network yang dilakukan pada trasnport atau network layer?

QR2 : bagaimana proses steganografi yang dilakukan pada transport atau network layer?

QR3: apakah masih terdapat kemungkinan pengembangan steganografi dalam network layer?

4. PELAKSANAAN

Tahapan ini adalah pelaksanaan dari SLR. Pada fase ini beberapa langkah dilakukan seperti terlihat pada gambar 2.



Gambar 2. Proses conducting SLR

Pada tahap pertama dalam conducting yang dilakukan adalah pelaksanaan strategi pemilihan literatur, yaitu diawali dengan pemilihan keyword dan sumber literatur. Sumber literatur yang digunakan adalah database artikel hasil penelitian yang terdapat pada laman scholar.google.com. pada proses pencarian literatur dibatasi pada artikel dalam bentuk jurnal dan proceedingconference dengan tahun publikasi 2015 hingga threequarter 2019. Setelah melakukan penentuan sumber dan pembatasan pencarian, langkah selanjutnya adalah menentukan keyword yang kemudian dilanjutkan dengan filtering literatur. Tahapan filteringiteratur ini dilakukan dengan cara membaca judul dan abstrak yang relevan dengan topik.

Dalam SLR ini, proses pencarian artikel dilakukan dengan menggunakan beberapa keyword. Keyword pertama adalah “steganogrpahy in socketprogramming”, yang dalam laman pencarian menghasilkan 345 hasil. Pada pencarian pertama, setelah dilakukan pembacaan judul dan abstrak dihasilkan 14 artikel yang dukup sesuai dan dapat didownloadsecarpenuh.Term kedua adalah “steganographysocketprogramming” yang menampilkan 261 artikel. Pada pencarian kedua dihasilkan 14 artikel yang dapat didownload penuh.Dan term ketiga adalah “steganograhy in transport layer”, pada pencarian ketiga didapatkan 20 artikel yang dapat didownload secara penuh. Sehingga didapatkan artikel sejumlah 48 dengan relevansi berdasar judul dan abstrak.

Pada fase qualityasesment, pertama dilakukan pencarian kualitas artikel berdasarkan jurnal yang memuatnya. Proses ini dilakukan dengan mengakses laman scimagojr.com untuk melihat kualitas dari jurnal yang memuat artikel yang diperoleh. Dalam fase ini dari 48 artikel, 40 adalah termuat dalam jurnal dan 8 termuat dalam proceedingconference. 42 artikel jurnal setelah dilakukan pencarian dalam laman scimagojr.com, didapatkan hasil 4 artikel dalam jurnal dengan kualifikasi Q1, 2 artikel dalam jurnal Q2, 4 artikel dalam jurnal Q3, 4 artikel dalam jurnal Q4 dan 28 artikel dalam jurnal yang tidak dikenal oleh schimagojr.com. tabel1 memberikan sebaran kualitas artikel berdasarkan peringkat jurnal dalam schimagojr.com.

Tabel1. Paper’sQualifications

	JournalQualification					Total
	Q1	Q2	Q3	Q4	Unknown	
Paper’sonJournal	4	2	4	4	26	40
ProceedingConference	-	-	-	-	-	8

Langkah selanjutnya dalam qualityasessment adalah melakukan sintesa terhadap artikel yang didapatkan dengan membaca secara keseluruhan artikel sehingga sesuai dengan topik dan questionresearch yang ditentukan.Hasil pada fase ini adalah terdapat 30 artikel yang cukup relevan dan terdapat 12 artikel yang relevan terhadap questionreaearch. Tabel 2 akan memberikan penilaian terhadap relevansi artikel terhadap topik dan questionresearch.

Tabel 2. Relevansi artikel terhadap topik

No.	Paper's Index	Qualification	Discussion		
			Cryptography	Steganography	Relevantwith Transport / Network Layer
1	[4]	-	Y	Y	-
2	[1]	-	Y	Y	Y
3	[5]	-	-	-	Y
4	[6]	-	Y	Y	Y
5	[2]	-	-	Y	Y
6	[3]	Q4	-	Y	Y
7	[7]	Q3	Y	-	Y
8	[8]	Q4	Y	-	Y
9	[9]	-	-	Y	Y
10	[10]	-	Y	-	Y
11	[11]	Q1	-	Y	Y
12	[12]	-	Y	Y	Y
13	[13]	-	Y	-	Y
14	[14]	-	-	Y	-
15	[15]	-	Y	Y	-
16	[16]	-	-	Y	-
17	[17]	-	-	Y	-
18	[18]	-	-	Y	-
19	[19]	-	Y	-	-
20	[20]	Q1	-	Y	-
21	[21]	-	-	-	-
22	[22]	-	Y	Y	-
23	[23]	-	Y	Y	-
24	[24]	Q1	Y	-	-
25	[25]	-	Y	-	-
26	[26]	Q1	-	-	-
27	[27]	Q3	-	-	-
28	[28]	Q1	-	-	-
29	[29]	Q2	-	Y	-
30	[30]	Q3	-	Y	-

Keterangan simbol : "Y" berarti artikel membahas tentang perihal sesuai kolom, "-" berati artikel tidak membahas perihal sesuai kolom.

5. PEMBAHASAN

Dalam diskusi akan menjabarkan hasil SLR untuk menjawab QuestionResearch

QR1 : apakah terdapat kegiatan penelitian tentang stegaografi dalam network yang dilakukan pada trasnport atau network layer?

Dalam SLR yang dilakukan, terdapat 12 artikel yang relevan sesuai dengan topik pembahasan dan pertanyaan pada researchquestion. Dalam paper ini terdapat penelitian pengamanan data pada transportlayer atau netowork layer. Artikel yang melakukan penelitian pengamanan data menggunakan steganografi, kriptografi maupun keduanya dengan melakukan proses pada transport layer sejumlah 8 artikel, 1 artikel melakukan proses pengamanan data pada network layer dan 3 artikel melakukan studi pengamatan terhadap mekanisme pengamanan data pada jalur komunikasi.

Tabel 2 memberikan gambaran bahwa perkembangan pengamanan data dalam network layer dilakukan dengan menggunakan teknik kriptografi atau steganografi. Terdapat penelitian yang menggunakan kombinasi kriptografi dan steganografi untuk memberikan kemamanan secara berlapis[1][6][12].

QR2 : bagaimana proses steganografi yang dilakukan pada transport atau network layer?

Proses pengembangan pengamanan data dengan menggunakan steganografi mayoritas dilakukan secara umum dan hanya terbatas pada lapisan aplikasi. Pada artikel yang di dapatkan terdapat beberapa penelitian dalam bentuk study. Diantaranya melakukan pengamatan terhadap pengembangan steganografi dalam physical layer atau link layer dengan mengusulkan modifikasi paket dan timingpada pengiriman dengan memberikan waktu delay[2]. Pengamatan lain melakukan pengamatan keamanan pada jaringan ad-hoc yang mengusulkan untuk dapat ditambahkan sebuah mekanisme untuk pertukaran kunci serta melakukan pengamanan data dengan teknik kriptografi [10]. Sebagai alat monitoring aliran paket data pada media transmisi sebuah studi menggunakan NS3 untuk melakukan pemantauan bentuk paket yang terkirim dalam IPv4 [5].

Mayoritas pengembangan steganografi yang dilakukan pada network lebih cenderung pada lapisan transport. Secara umum disebutkan bahwa pengamanan data dilakukan dengan teknik enkripsi dan steganografi, meskipun diterapkan apdasocket[8].Sebuah penerapan dengan menggunakan teknik enkripsi RSA untuk membentuk sebuahcipher dan kemudian mentransform menjadi biner dan dipecah menjadi 20 bit per paket[1]. Penelitian lain melakukan modifikasi pada StreamTransport ControlProtocol (STCP) dengan melakukan multi level security menggunakan secretmatrix, kunci rahasia, hiddensignature dan steganography[6]. Modifikasi pengiriman lain melalui transport layer dilakukan dengan melakukan permutasi paket menggunakan tabel yang telah disepakati pengirim dan penerima[3]. Pengurangan ukuran paket juga dilakukan untuk mencegah kemacetan pengiriman dalam transmisi [7]. Pendekatan lain adalah menggunakan header dalam TCP/IP sebagai cover, namun hal ini hanya mampu menampung 4 karakter dalam setip pengiriman komunikasi [9]. Usulan lain adalah dengan melakukan proses streaming data yang dilakukan secara serial dengan menggunakan frameworkcrosslayer[11].

Proses pengamanan data masih didominasi dengan menerapkan mekanisme kriptografi dan steganografi. Meskipun diterapkan dalam modifikasi ukuran paket, penyematan dalam header, namun pesan yang dirahasiakan yang tersemat masih mengalir pada jalur komunikasi.sebuah penelitian menyarankan untuk dilakukan sebuah pengamatan lalulintas data guna melakukan analisa anomali besaran paket [13].

QR3: apakah masih terdapat kemungkinan pengembangan steganografi dalam network layer?

Pengamanan data dalam jalur komunikasi diperkirakan akan terus dilakukan. Hal ini beberapa usulan yang dilaporkan pada penelitian sebelumnya yaitu dengan melakukan

penggabungan beberapa teknik kriptografi dan steganografi[4][8], modifikasi algoritma[11], modifikasi ukuran paket[1] [7], meyisipkandalam coverheader[9], penambahan digital signature[12] serta melakukan pengamatan pada lalu lintas data juga masih diperlukan untuk melihat anomali streaming data [13].

6. KESIMPULAN

Dari pelaksanaan SLR, beberapa kesimpulan tentang perkembangan teknik steganografi dalam lapisan network sebagai berikut :

Pengembangan pengamanan data menggunakan steganografi dikombinasikan dengan kriptografi untuk memberikan keamanan data, keaslian dan integritas data sertamemberikan kepercayaan informasi bagi penerima.

Pengembangan steganografi juga dilakukan dengan melakukan modifikasi pada ukuran paket, modifikasi dengan pemberian penambahan waktu jeda pengiriman dan penggunaan header sebagai cover data pesan.

Meskipun demikian mekanisme steganografi yang dilakukan secara mayoritas masih tetap mengalirkan data pesan melalui media transmisi, meskipun pesan tersebut sudah dirahasiakan dan memiliki cover.

Untuk mendukung bentuk pengamanan data berjalan melalui media komunikasi, lebih jauh penulis akan mengembangkan sebuah konsep melakukan pengembangan pengamanan data berjalan dengan melihat kondisi lalu lintas data guna pengambilan keputusan dalampemecahan ukuran paket sebelum dilakukan pengiriman melalui media transmisi.

DAFTAR PUSTAKA

[1] S. Bobade dan R. Goudar, "Secure Data Communication Using Protocol Steganography in IPv6," dalam *IEEE: 2015 International Conference on Computing Communication Control and Automation*, 2015.

[2] J. O. Seo, S. Manoharan dan A. Mahanti, "A Discussion and Review of Network Steganography," dalam *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing*, 2016.

[3] F. X. Peng, S. H. Jing dan G. H. Rong, "A New Network Steganographic Method Based in The Transverse Multi-Protocol Collaboration," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 8, no. 2, pp. 445-459, 2017.

[4] R. Hedge dan T. H. Sreenivas, "Steganography in Ad Hoc Network," *International Journal of Computer Science and Information Technologies,* vol. 6, no. 6, pp. 5405-5408, 2015.

[5] H. Kheddar dan M. Bouzid, "Implementation of Steganographic Method Based in IPv4 Identification Field over NS-3," *International Journal of Engineering Research and Applications,* vol. 5, no. 3, pp. 44-48, 2015.

[6] P. Venkadesh, J. P. M. Dhas dan S. V. Divya, "Techniques to enhance security in SCTP for multi-homed networks," dalam *IEEE : 2015 Global Conference on Communication Technologies (GCCT)*, 2015.

[7] P. Gulia dan Reena, "A Novel Technique of Security Improvement in Ad-hoc Network by using FTP," *International Journal of Applied Engineering Research,* vol. 12, no. 17, pp. 6658-6662, 2017.

[8] S. Dalal dan S. Devi, "Security Framework against Denial of Service Attacks in Wireless Mesh Network," *Global Journal of Pure and Applied Mathematics,* vol. 13, no. 2, pp. 829-837, 2017.

[9] J. M. Kadhim dan A. E. Abed, "Steganography Using TCP/IP's Sequence Number," *Al-Nahrain Journal of Science,* vol. 20, no. 4, pp. 102-108, 2017.

[10] Reena dan P. Gulia, "Review of Security in AD-HOC Network Using FTP," *Advances in Computational Sciences and Technology,* vol. 10, no. 5, pp. 1417-1426, 2017.

[11] F. Shamieh dan X. Wang, "Dynamic Cross-Layer Signaling Exchange for Realtime and On Demand Multimedia Streams," *IEEE Transactions On Multimedia,* vol. 17, no. 10, pp. 1-12, 2018.

[12] I. Ruban, N. L. Chuiko, V. Mukhin, Y. Kornaga, I. Grishko dan A. Smirnov, "The Method of Hidden Terminal Transmission of Network Attack Signatures," *International Journal Computer Network and Information Security,* vol. 4, pp. 1-9, 2018.

[13] B. Troegeler dan P. Watters, "Steganographic Transports: A Vector for Hidden Secret Internets?," dalam *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications*, 2018.

[14] K. Nair, K. Asher dan J. Joshi, "Implementing Semi-Blind Image Steganography with Improved Concealment," dalam *IJCA Proceedings on International Conference on Computer Technology*, 2015.

[15] S. Nagendrudu dan V. R. Reddy, "Integration of BPCS Steganography and Visual Cryptography for Secure e-Pay," *International Journal on Computer Science Engineering and Technology,* vol. 5, no. 6, pp. 162-165, 2015.

[16] G. R. Manujala dan A. Danti, "Embedding Multiple Images in A Single Image using Bit Plane Complexity Segmentation (BPCS) Steganography," *Asian Journal of Mathematics and Computer Research,* vol. 2, no. 3, pp. 136-142, 2015.

[17] I. G. Raman dan K. P. Kaliyamurthie, "An Adaptive Data Hiding Scheme for Domain Based Secret Data in Random Order to Increase Steganography Using IWT," *International Journal Advanced Networking and Applications,* vol. 6, no. 5, pp. 2464-2467, 2015.

[18] R. Kumar dan M. Dhiman, "Secured Image Transmission Using a Novel Neural Network Approach and Secret Image Sharing Technique," *International Journal of Signal Processing, Image Processing and Pattern Recognition,* vol. 8, no. 1, pp. 161-192, 2015.

[19] O. S. Adebayo, M. Olalere dan J. N. Ugwu, "Implementation of N-Cryptographic Multilevel Cryptography Using RSA and Substitution Cryptosystem," *MIS Review,* vol. 20, no. 2, pp. 57-76, 2015.

[20] W. Mazurczyk dan L. Caviglione, "Steganography in Modern Smartphones and Mitigation Techniques," *IEEE Communications Surveys & Tutorials,* vol. 17, no. 1, pp. 334-357, 2015.

[21] S. A dan K. M, "Design and Implementation of Standby Power Saving Smart Socket with Wireless Sensor Network," dalam *2nd Internasional Conference on Intelegent Computing, Communication & Convergance*, 2016.

[22] S. Akolkal, Y. Kokulwar, A. Neharkar dan D. Pawar, "Secure Payment System using Steganography and Visual Cryptography," *Internasional Journal of Computing and Technology,* vol. 3, no. 1, pp. 58-61, 2016.

[23] S. S. Brar, "Double Layer Image Security System using Encryption and Steganography," *International Journal Computer Network and Information Security,* vol. 3, pp. 27-33, 2016.

[24] K. Morovati, A. Ghorbani dan S. Kadam, "A network based document management model to prevent data extrusion," *Computers & Security,* vol. 59, pp. 71-91, 2016.

[25] D. Demirol, R. Das dan G. Tuna, "An android application to secure text messages," dalam *IEEE 2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, 2017.

[26] E. A. Hassan, H. Shareef, M. M. Islam, E. Wahyudie dan A. A. Abdrabou, "Improved Smart Power Socket for Monitoring and Controlling Electrical Home Appliances," *IEEE Access,* vol. 6, pp. 49292-49305, 2018.

[27] R. Rahim, J. Simarta, A. Purba, M. A. Prayogi, A. Sapta, O. K. Sulaiman, M. A. Sembiring, R. Ramadhani, A. R. S. Tambunan, H. Hasdiana, P. Simbolon, S. Aisyah, J. Juliana dan S. Suharman, "Internet based remote desktop using INDY and socket component," *Internasional Journal of Engineering & Technology,* vol. 7, no. 29, pp. 44-47, 2018.

[28] C. Wijayarathna dan N. A. G. Arachchilage, "Why Johnny Can't Develop a Secure Application? A Usability Analysis of Java Secure Socket Extension API," *Computers & Security,* vol. 80, pp. 54-73, 2018.

[29] G. Xin, Y. Liu, Y. Yang dan Y. Cao, "An Adaptive Audio Steganography for Covert Wireless Communication," *Security and Communication Networks,* vol. 2018, pp. 1-10, 2018.

[30] Y. A. Issa, M. A. Ottom dan A. Tamrawi, "eHealth Cloud Security Challenges: A Survey," *Journal of Healthcare Engineering,* vol. 2019, pp. 1-15, 2019.