Aplikasi Graf untuk Pendeteksian Spammer Email

Natan (13513070)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
natanelia@students.itb.ac.id

Abstrak*—Layanan email telah hadir bertahun-tahun lamanya. Kini penggunaan layanan email tetap menjamur dengan jumlah pengguna yang semakin banyak. Sayangnya, pihak-pihak tertentu memanfaatkan popularitas layanan tersebut untuk hal-hal negatif dalam bentuk spam. Oleh sebab itu dibutuhkan sebuah sistem yang dapat mendeteksi spam, sehingga bisa dipisahkan dari email lainnya. Salah satu metode yang bisa digunakan adalah dengan memanfaatkan graf sosial yang dibentuk dari aktivitas penggunaan layanan email. Pada makalah ini akan dibahas bagaimana metode graf sosial tersebut dapat diimplementasikan pada sistem pendeteksian spam. Dengan demikian, penyebaran spam dapat dibatasi secara maksimal.

***Keywords*— graf sosial, email, pendeteksian spam, keamanan**

I. PENDAHULUAN

Masyarakat dunia kini sudah tidak asing lagi dengan surat elektronik atau yang lebih dikenal dengan sebutan email. Walaupun telah banyak diciptakan layanan komunikasi digital lainnya, email tetap menjadi salah satu pilihan masyarakat dunia hingga saat ini. Hal ini tidak terlepas dari sifat email yang dianggap lebih resmi, universal, dan jelas dalam menyampaikan pesan digital, serta masih terus dikembangkan hingga kini. [1]

Perilaku mengirimkan email ke pengguna lainnya dapat dikategorikan sebagai relasi sosial. Ketika pengguna mengirimkan email ke pengguna lainnya, ada sebuah relasi yang dibangun. Ketika terjalin aksi saling berbalas email, relasi timbal-balik terbentuk. Ketika ada aksi saling mengirim email di antara beberapa orang, relasi komunitas terbentuk. Relasi ini dapat direpresentasikan sebagai graf yang menyatakan pengguna sebagai simpul dan aktivitas mengirimkan email sebagai sisi.

Dengan melakukan observasi terhadap aktivitas pertukaran email dalam jangka waktu tertentu, penyedia layanan email dapat membuat graf yang merepresentasikan pola pengiriman email dan relasi yang abnormal dalam sebuah komunitas. Adanya relasi yang abnormal menandakan bahwa ada pengguna yang mengancam keamanan pengguna lainnya. Dalam sistem keamanan email, graf sosial para pengguna email menjadi salah satu elemen penting dalam memerangi email jahat atau yang biasa disebut dengan *spam*.

II. TEORI GRAF

Graf adalah sebuah cara untuk merepresentasikan objek-objek diskrit dan relasinya dengan menggunakan simpul dan sisi penghubung. Graf telah diaplikasikan dalam banyak hal seperti pembangunan jalan lintas kota, distribusi produk bisnis, jaringan internet, susunan senyawa kimia, gambar digital berbasis vektor, dan pencitraan tiga dimensi. Bentuk graf dari suatu data memungkinkan data yang berhubungan dengan konektivitas dapat lebih mudah dimengerti dan diolah. [2]

A. Definisi Graf

Sebuah graf G = (V, E) terdiri atas V = $\{v_1, v_2, \ldots, v_n\}$, yang merupakan himpunan simpul (*vertices*) tidak kosong, dan E = $\{e_1, e_2, \ldots, e_n\}$, yang merupakan himpunan sisi (*edges*). Setiap sisi dalam graf menghubungkan sepasang simpul. [2]

B. Jenis Graf

Berdasarkan ada tidaknya gelang atau sisi ganda pada suatu graf, maka graf dapat digolongkan menjadi dua, yaitu:

1. Graf sederhana: graf yang tidak mengandung gelang maupun sisi-ganda.
2. Graf tak-sederhana: graf yang mengandung sisi ganda atau gelang.

Berdasarkan banyaknya simpul, graf dapat digolongkan menjadi dua yaitu:

1. Graf berhingga: graf dengan banyak simpul terhingga.
2. Graf tak-berhingga: graf dengan banyak simpul tak terhingga.

Berdasarkan ada tidaknya arah pada sisi graf, maka graf dapat digolongkan menjadi dua yaitu:

1. Graf tak-berarah: graf tanpa sisi berarah.
2. Graf berarah: graf yang semua sisinya memiliki arah.

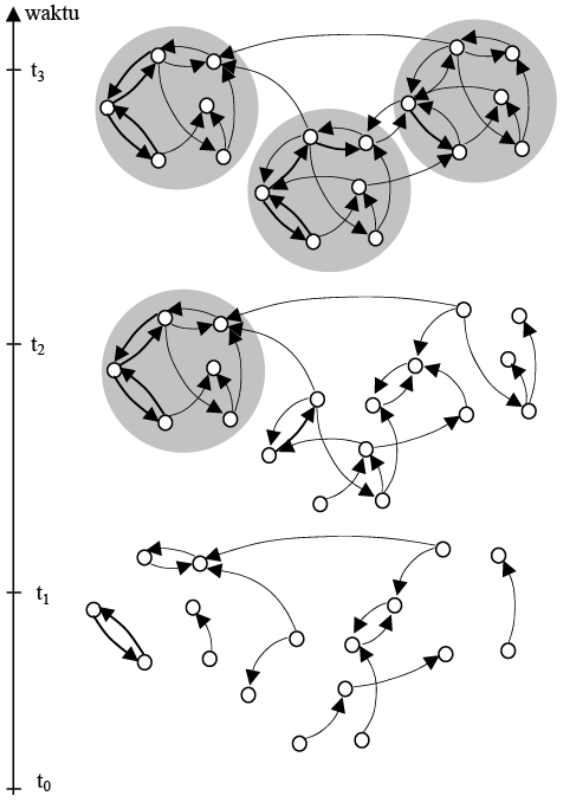
Suatu graf dapat dilengkapi dengan bobot pada tiap sisinya untuk memberikan informasi tambahan. Misalnya, pada kasus graf pembuatan jalan antarkota, sisi-sisi yang menghubungkan tiap kota dapat memiliki bobot harga pembuatan jalan tersebut. [3]

C. Graf Sosial

Graf sosial adalah graf berarah yang merepresentasikan relasi sesungguhnya dalam suatu komunitas pada jangka waktu tertentu. Graf tersebut berubah seiring waktu untuk menandakan relasi yang sekarang sedang terjadi antar anggota komunitas tersebut. Graf sosial didefinisikan sebagai $G_t = (V_t, E_t)$, yaitu suatu graf berarah yang terbentuk setelah jangka waktu yang ke-t. V_t adalah himpunan simpul yang merepresentasikan anggota komunitas sosial, sedangkan E_t adalah himpunan sisi berarah yang merepresentasikan hubungan antar anggota komunitas tersebut.

Sisi-sisi graf pada sebuah jaringan sosial dapat memiliki bobot yang menunjukkan kekuatan suatu relasi. Faktor-faktor yang dapat dijadikan sebagai nilai bobot adalah hubungan keluarga, tingkatan umur, kesamaan tempat kerja atau sekolah, kesamaan daerah, dan kesamaan grup.

Suatu relasi sosial dapat dikatakan terjalin dengan baik apabila relasi tersebut secara terus-menerus terjadi secara timbal-balik pada graf G_t (t = 1, 2, 3, …). Apabila pada jangka waktu yang panjang suatu simpul A hampir selalu dihubungkan dua sisi timbal-balik dengan suatu simpul B, dapat dikatakan A dan B memiliki relasi sosial yang baik. Namun apabila dalam jangka waktu yang panjang simpul A dan simpul B hanya dihubungkan sebuah simpul berarah dari A ke B, dapat dikatakan hubungan simpul A dan B hanya terjadi sebelah pihak dan tidak terjalin relasi yang baik. [4]



Gambar 2.1. Graf sosial dari jangka waktu t_1 sampai t_3. Bagian yang dilingkari menandakan relasi sosial yang terjalin dengan baik.

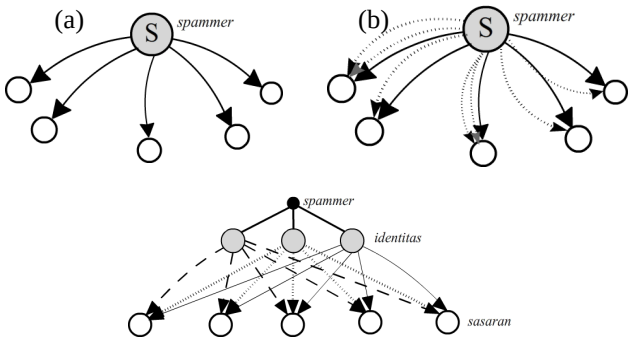
III. PERILAKU SPAMMER PADA LAYANAN EMAIL

Spam adalah email yang tidak dikehendaki penerimanya dan dikirimkan sekaligus ke banyak pengguna lainnya. Isi dari email spam kerap mengandung tautan ke situs yang mengandung hal negatif seperti judi, pornografi, bahkan *virus* dan *malware* yang bisa saja ter-*install* secara otomatis begitu pengguna mengakses tautan tersebut. Email-email tersebut harus dipisahkan dari email-email biasa untuk kepentingan keamanan pengguna [5].

Untuk melakukan penyortiran terhadap email spam, dibutuhkan suatu mekanisme yang dapat membedakan email asli dan email spam. Dengan mengamati pola pengiriman email, kita dapat membuat graf berpola yang dapat menunjukkan adanya anomali perilaku pengirim email. Tentunya semakin lama kita melakukan pengamatan, akan didapatkan data yang lebih akurat dalam membedakan perilaku spammer dan pengguna reguler.

Berdasarkan cara beroperasinya, spammer dapat digolongkan ke dalam 3 jenis, yaitu:

1. Only-Once One-Face (OOOF): spammer hanya mendistribusikan email spam sekali dengan satu alamat email.
2. Multiple-Times One-Face (MTOF): spammer mengirimkan spam berkali-kali dengan satu alamat email.
3. Multiple-Times Multiple-Face (MTMF): spammer mengirimkan spam berkali-kali dengan identitas yang berbeda-beda. Hal ini dapat dicapai dengan membuat banyak alamat email atau merekayasa bagian "From: " pada *header* email. [5]



Gambar 3.1. Graf pola perilaku spammer: (a) OOOF; (b) MTOF; (c) MTMF

Ada beberapa pola perilaku spammer yang dapat diamati. Pertama, spammer mengirimkan email ke banyak pengguna lain sekaligus. Kedua, email spam biasanya tidak menuntut balasan. Dengan kata lain, pengguna tidak akan membalas email spam. Ketiga, spammer tidak pernah mengirimkan email tanpa tautan atau attachment. Ketiga hal ini dapat dijadikan acuan dalam menentukan dan memblokir spammer. Sebenarnya masih banyak pola-pola spam lainnya, namun penulis hanya ingin

mencantumkan pola yang berhubungan dengan makalah ini. [6]

IV. METODE PENDETEKSIAN SPAMMER

Tingkat keamanan sebuah layanan email akan sangat tergantung pada kemampuan layanan dalam memisahkan email spam dari email reguler. Untuk itu diperlukan metode-metode pendeteksian spam yang komprehensif agar mampu dengan baik menentukan apakah suatu email spam atau tidak. Ada banyak solusi yang saat ini sudah diterapkan, kebanyakan memfokuskan perhatian pada analisa konten email. Analisa konten email dapat dilakukan dengan memeriksa tautan-tautan yang disisipkan, memeriksa kata-kata yang digunakan, dan ketidakwajaran nama pengirim email. Selain itu, email spam juga dapat dideteksi melalui metode daftar hitam atau *blacklisting*, yakni dengan secara langsung menetapkan email yang dikirimkan dari alamat mencurigakan sebagai spam. Metode *blacklisting* dapat dimodifikasi sedemikian rupa agar dapat secara otomatis menentukan apakah pengirim email patut dicurigai sebagai spammer. Penulis akan membahas metode *blacklisting* dengan cara mengamati perilaku pengguna yang mencurigakan.

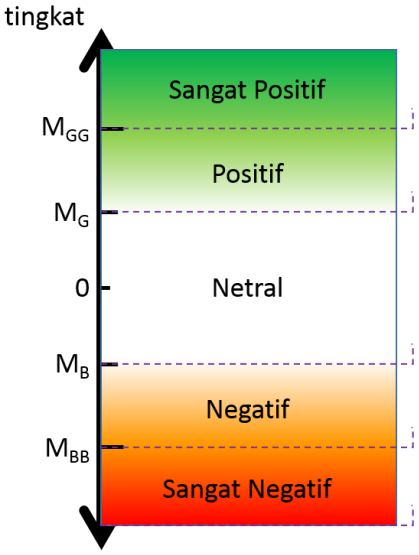
Sebuah sistem pendeteksi spam dengan mengamati pola perilaku pengguna dapat dikatakan berfungsi secara efektif apabila sistem dapat menemukan anomali perilaku spammer dengan cepat dan tepat. Kecepatan deteksi berbicara mengenai rentang waktu yang dibutuhkan untuk memutuskan apakah sebuah email berasal dari spammer, sedangkan ketepatan deteksi berbicara mengenai berapa persen email spam yang terdeteksi sebagai spam dan seberapa minimal kesalahan sistem mendeteksi email reguler sebagai spam. Kedua faktor ini sangatlah penting dalam menentukan variabel-variabel suatu sistem pendeteksi spam.

Sistem yang dibangun akan mencatat pola perilaku pengguna sekarang yang dipengaruhi oleh perilaku sebelumnya dalam bentuk angka. Kemudian sistem akan mengklasifikasikan pengirim email sebagai spammer berdasarkan nilai angka tersebut. Pola perilaku didefinisikan sebagai G_i dengan i = 1, 2, 3, …, n. Dari G_i dapat dihitung G_{TOTAL} melalui rumus:

$$G_{TOTAL} = \sum_{i=0}^{n} G_i \qquad (1)$$

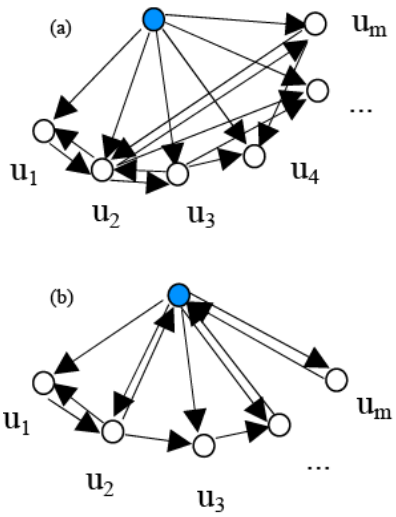
Batas nilai suatu pola perilaku dikatakan sebagai positif atau negatif masing-masing ditandai dengan M_G dan M_B. Apabila nilai $G_{TOTAL} < M_B$, pengirimnya dapat dicurigai sebagai spammer. Klasifikasi-klasifikasi yang digunakan dapat dilihat pada gambar 4.1.

Klasifikasi pengguna email dilakukan dengan memanfaatkan graf sosial dari pengguna tersebut. Sistem akan mencatat semua aktivitas pengguna per jangka waktu t. Dari tiap jangka waktu tersebut akan didapati pengguna tersebut telah mengirimkan dan mendapatkan email dari siapa saja. Seperti yang telah disebutkan sebelumnya, pengguna reguler tidak pernah atau jarang membalas email spammer. Dengan kata lain, apabila interaksi



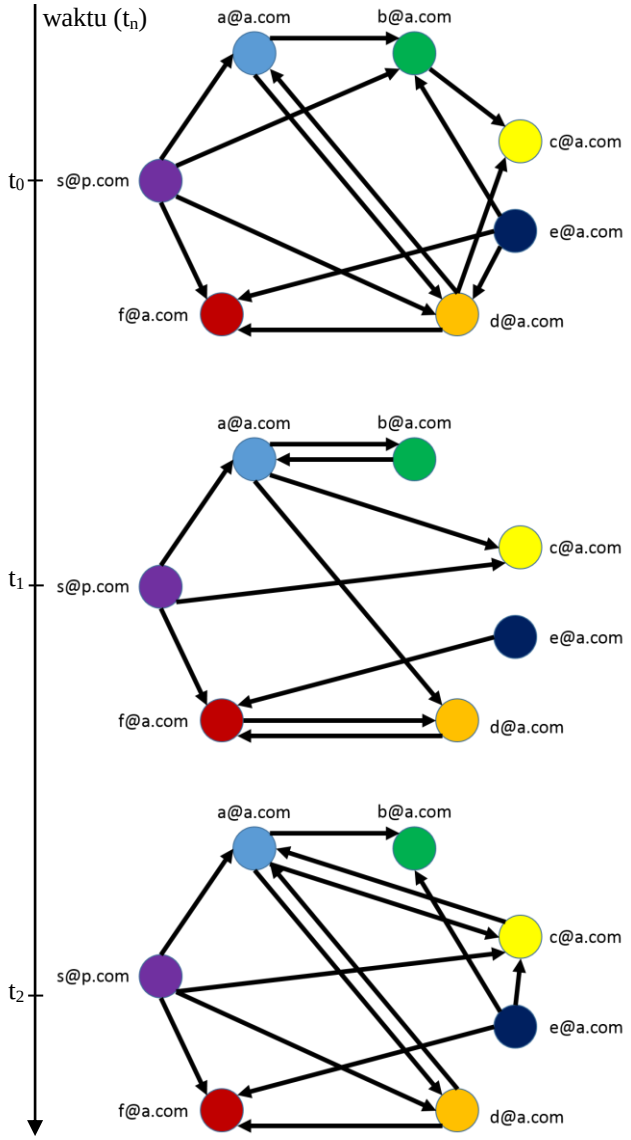
Gambar 4.1. Klasifikasi perilaku pengirim email.

mengirim email hanya dilakukan dari satu pihak secara terus menerus oleh pengguna tertentu, pengguna tersebut dapat dicurigai sebagai spammer. Kita bisa membandingkan perilaku spammer melalui gambar 4.2. Pada bagian (a) dapat dilihat seorang pengguna mengirimkan email ke banyak orang sekaligus. Namun ia tidak dapat dikatakan sebagai spammer karena ada sejumlah orang yang juga mengirimkan email balasan kepadanya. Ia dapat dikatakan memiliki relasi sosial yang kuat karena ada hubungan timbal-balik yang membuatnya tidak dicurigai sebagai spammer. Sedangkan pada bagian (b) dapat dilihat seorang pengguna juga mengirimkan email ke banyak pengguna dalam satu waktu. Pengguna lainnya tidak pernah mengirimkan email balasan, walau mereka berinteraksi satu sama lain. Maka, pengguna yang hanya berinteraksi satu arah tersebut dapat dicurigai sebagai spammer.



Gambar 4.2. Graf pola perilaku pengguna email: (a) perilaku spammer; (b) perilaku penguna reguler.

Dalam suatu layanan email percobaan dengan *domain* "@a.com" didapati graf sosial dari t_0 hingga t_2 seperti pada gambar 4.3.



Gambar 4.3. Sampel graf sosial layanan email pada t_0-t_2.

Sistem mengadopsi nilai batas M_G = +20 dan M_B = -5. Setiap pengiriman email akan menghasilkan G_i = -1, sedangkan setiap penerimaan email akan menghasilkan G_i = +5 Apabila sistem mengeksekusi pendeteksian spam berdasarkan t_0-t_2, akan didapati tabel 4.1.

Tabel 4.1. Hasil analisa graf sosial t_0-t_2

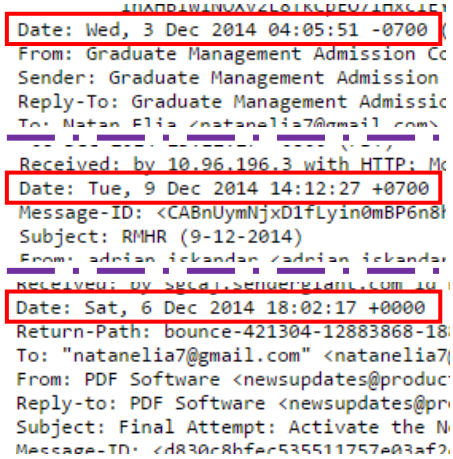
Email	G_0	G_1	G_2	G_{TOTAL}
a@a.com	+8	+7	+12	+8
b@a.com	+14	+4	+4	+16
c@a.com	+4	+10	+14	+28
d@a.com	+12	+9	+8	+29
e@a.com	-3	-1	-3	-7
f@a.com	+15	+14	+15	+44
s@p.com	-4	-3	-4	-11

Melalui tabel 4.1 didapati bahwa s@p.com dan e@a.com memiliki G_{TOTAL} masing-masing -11 dan -7. Keduanya memenuhi syarat $G_{TOTAL} < M_B$ sehingga sistem mengklasifikasikan s@p.com dan e@a.com dicurigai sebagai spammer.

Pendeteksian spam dengan hanya menggunakan graf sosial di atas cukup meyakinkan, namun belum tentu dapat menetapkan spammer dengan tepat. Oleh sebab itu, sistem dapat memperlengkapi graf sosial tersebut dengan bobot sisinya. Semakin tinggi bobotnya, semakin dipercaya suatu alamat email. Dalam hal ini, saat sistem mendapati sebuah alamat email dicurigai sebagai spammer, sistem akan memeriksa bobot sisi alamat email tersebut. Ada beberapa faktor yang bisa dijadikan acuan untuk menentukan nilai bobot suatu sisi, yaitu:

1. *Kesamaan domain*: *domain* alamat email yang sama antara pengirim dan penerima email dapat melambangkan bahwa email tidak pantas dicurigai sebagai spam. Misalnya, sangat jarang ditemui pengguna layanan Gmail dengan *domain* "@gmail.com" yang mengirimkan spam ke *domain* yang sama. Kesamaan *domain* selanjutnya didefinisikan dengan variabel *d*.
2. *Alamat email terdaftar di daftar kontak*: pengguna biasanya kesulitan untuk menghafalkan alamat email pengguna lainnya. Sebagai solusinya semua layanan email telah memberikan fasilitas daftar kontak (*address book*). Dalam hal ini, pengguna tidak pernah atau jarang sekali menyimpan alamat email spammer ke dalam daftar kontak mereka. Sebaliknya, email-email penting akan dimasukkan ke daftar kontak, sehingga darinya dapat ditentukan bahwa alamat yang ada di dalam daftar kontak tidak pantas dicurigai sebagai spam. Terdaftarnya alamat *email* pengirim dalam daftar kontak penerima selanjutnya akan didefinisikan dengan variabel *a*.
3. Kesamaan domisili: Spammer biasa memiliki data alamat email secara random tanpa memerhatikan lokasi pemilik email reguler berada. Tujuannya kerap hanya bermaksud menyebarkan *malware* atau mencuri data pengguna. Dalam hal ini, pengirim email yang memiliki domisili berbeda dari penerima lebih dicurigai sebagai spammer. Untuk bisa mengetahui domisili pengirim, sistem hanya bisa memanfaatkan *header* email yang dikirimkan. *Header* email mengandung alamat IP pengirim, alamat IP penerima, waktu kirim, dan zona waktu pengirim. Penulis telah menganalisa lebih dari 10 email reguler dan spam, dan menemukan bahwa alamat IP sebagian besar telah mengalami *routing* sehingga tidak secara akurat merepresentasikan domisili pengirim. Oleh sebab itu, sistem pendeteksi hanya dapat mengenali domisili dari zona waktu pengirimnya. Apabila zona waktunya sama, pengirim lebih tidak pantas dicurigai sebagai spammer. Hal yang perlu

diperhatikan di sini adalah cara penentuan bobot yang melibatkan kesamaan domisili kurang efektif diterapkan pada pengguna email yang berdomisili di negara-negara sumber pengirim spam, yang dalam hal ini Indonesia tidak termasuk di dalamnya. Selanjutnya kesamaan domisili akan didefinisikan dengan variabel *p*.



Gambar 4.4. Contoh cuplikan *header* email yang ditandai dengan zona waktu berbeda.

Dengan menggabungkan tiga faktor di atas, dapat dibuat sebuah rumus untuk menentukan bobot sisi graf sosial (s). Berikut adalah rumus yang dapat digunakan:

$$s = xd + ya + zp \qquad (2)$$

dengan s sebagai bobot sisi graf, d sebagai nilai kesamaan domain, a sebagai nilai terdaftarnya alamat email pada daftar kontak, *p* sebagai nilai kesamaan domisili berdasarkan zona waktu, *x*, *y* dan *z* sebagai variabel besarnya pengaruh faktor d, a, dan p terhadap bobot sisi. Variabel *d*, *a*, dan *p* bernilai 0 (*false*) atau 1 (*true*) tergantung dari berlaku atau tidaknya faktor tersebut. Untuk variabel x, y, z direkomendasikan memiliki nilai yang memenuhi syarat $x \geq y > z$ berdasarkan tingkatan pengaruh yang paling menentukan. Sistem yang dibuat dapat menentukan nilai *x*, *y*, dan *z* menyesuaikan dengan layanan emailnya.

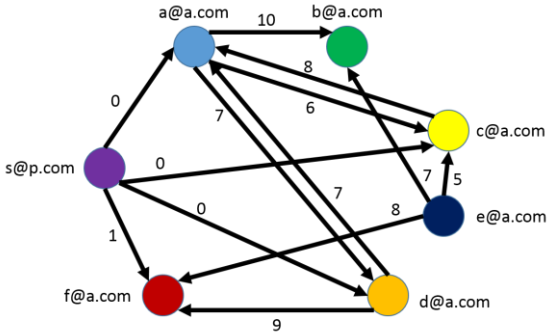
Sebagai contoh, penulis mengimplementasikan syarat email **bukan spam apabila** $s \geq 5$, dengan menggunakan nilai variabel berikut:

$$x = 5, \quad y = 3, \quad z = 2$$

Apabila didapati data aktivitas pertukaran email di t_2 seperti pada tabel 4.2, dapat dibuat graf sosial berbobot seperti pada gambar 4.5.

Tabel 4.2. Data penggunaan email pada t_2.

Pengirim	Penerima	Daftar Kontak	Zona Waktu Pengirim	Zona Waktu Penerima
a@a.com	b@a.com	true	+0700	+0700
a@a.com	c@a.com	false	+0700	-0600
a@a.com	d@a.com	false	+0700	+0700
d@a.com	f@a.com	true	+0700	+0000
s@p.com	a@a.com	false	+0000	+0700
s@p.com	c@a.com	false	+0000	-0600
s@p.com	d@a.com	false	+0000	+0700
s@p.com	f@a.com	false	+0000	+0000
c@a.com	a@a.com	true	-0600	+0700
d@a.com	a@a.com	false	+0700	+0700
e@a.com	b@a.com	false	+0700	+0700
e@a.com	d@a.com	false	+0700	-0600
e@a.com	f@a.com	true	+0700	+0000



Gambar 4.5. Graf sosial penggunaan email pada t_2.

Apabila sistem domain "*@a.com*" mengeksekusi pendeteksian spam berdasarkan graf sosial t_0-t_2 dengan mempertimbangkan bobot pada t_2, s@p.com akan dipastikan sebagai spammer sedangkan e@a.com akan dianggap pengguna reguler. Semua email dari e@a.com tidak dianggap sebagai spam karena tiap sisinya memenuhi $s \geq 5$. Dapat dilihat di sini bahwa pemberian bobot menghindari pengguna reguler dengan alamat email e@a.com dianggap juga sebagai spammer.

V. SIMPULAN

Sistem pendeteksi spam dengan menggunakan graf sosial dapat diterapkan di semua layanan email. Graf sosial akan terbentuk tiap jangka waktu tertentu. Karena tiap graf akan berkontribusi terhadap ketepatan deteksi spam, sistem ini akan semakin cerdas seiring berjalannya waktu.

Sistem yang dibuat pada makalah ini dapat digunakan sebagai dasar dalam pengembangan pendeteksian spam lebih lanjut. Variabel-variabel bebas pada sistem ini dapat dimodifikasi sedemikian rupa menyesuaikan dengan kondisi layanan email sesungguhnya untuk mengoptimalkan kecepatan dan ketepatan deteksi spam. Sistem ini juga dapat dikombinasikan dengan metode-metode pendeteksian spam lainnya, seperti sistem analisa konten email. Dengan demikian diharapkan layanan email dapat memisahkan spam dari email reguler secara sempurna.

VII. UCAPAN TERIMA KASIH

Pertama-tama penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada Tuhan yang Maha Esa atas hikmat dan waktu yang telah diberikan agar saya dapat menyelesaikan makalah ini. Penulis juga ingin berterima kasih kepada kedua orang tua penulis karena tanpa mereka, saya tidak akan bisa meraih pengetahuan sampai saat ini. Tak lupa penulis juga ingin mengucapkan terima kasih kepada Bapak Rinaldi Munir karena melalui pengajarannya, saya dapat mengerti konsep Matematika Diskrit dan teori graf yang menjadi dasar makalah ini.

REFERENSI

[1] http://blog.campaignmaster.co.uk/2013/05/16/5-reasons-why-email-isnt-going-anywhere, diakses pada tanggal 7 Desember 2014 pukul 18.32

[2] K.H. Rosen, *Discrete Mathematics and Its Applications* 6th Edition. New York: McGraw-Hill, 2007

[3] Munir, Rinaldi, *Matematika Diskrit, ed. 2. Bandung: Penerbit Informatika, 2003*

[4] S. Wasserman, K. Faust, *Social Network Analysis, Methods and Applications.* Cambridge University Press, 2007

[5] M.E.J. Newman, S. Forrest, J. Balthrop, "E-mail networks and the spread of computer viruses", *Physical Review* E 66, 035101(R). University of New Mexico, 2002

[6] P.O. Boykin, V. P. Roychowdhury, "Leveraging social networks to fight spam", *IEEE Computer*, April 2005

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 10 Desember 2014

Natan (13513070)