PROTOKOL KUNCI PUBLIK PADA KOMUNIKASI NIRKABEL

Dwinanto Cahyo – NIM : 13505025

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15025@students.if.itb.ac.id

Abstrak

Protokol untuk otentifikasi dan penggunaan kunci dalam lingkungan komunikasi nirkabel memiliki kebutuhan tersendiri. Generasi sistem nirkabel terbaru kemungkinan besar akan menggunakan protokol berbasiskan kunci publik. Terdapat sejumlah keputusan terhadap rancangan penting dalam memilih protokol yang akan digunakan. Makalah ini akan mengulas kebutuhan rancangan beserta sejumlah protokol kunci publik yang diajukan untuk komunikasi nirkabel. Kemudian akan dibahas sebuah protokol kunci publik yang diajukan.

***Kata kunci**:* keamanan, komunikasi nirkabel, kunci publik, protokol.

1. Pendahuluan

Dalam dunia dengan globalisasi dan perkembangan teknologi komunikasi yang semakin pesat, khususnya pada penyediaan layanan nirkabel, kebutuhan terhadap layanan keamanan akan lebih besar dan rumit dibandingkan dengan pada masa penggunaan teknologi digital dengan kabel. Untuk memenuhi kebutuhan tersebut, dikenal protokol dan algoritma kriptografi yang secara langsung maupun tidak turut berkembang seiring bidang penggunaannya yang semakin luas. Potensi bahaya terbesar gangguan keamanan adalah antara pengguna dan jaringan, analoginya adalah dalam suatu hubungan melalui radio. Keamanan yang terpenting dalam antarmuka tersebut adalah mencegah manipulasi akses ke sumber daya jaringan dan menjaga privasi pengguna.

Ketika sebuah kunci rahasia bersama terjalin antara dua entitas melalui suatu antarmuka, data digital suara dan informasi dapat dilindungi dengan enkripsi simetris dan mekanisme pemeriksaan. Fokus pembahasan dalam makalah ini adalah pada protokol untuk menciptakan sesi komunikasi dengan kunci simetris tersebut, termasuk mekanisme untuk mengenali dan memeriksa keaslian identitas pihak yang terlibat atau otentifikasi.

Protokol untuk otentifikasi yang digunakan untuk menciptakan sesi komunikasi pada teknologi digital saat ini bergantung pada sejumlah kunci permanen antara sesama pengguna dan jaringan yang berafiliasi dengan pihak masing-masing. Dengan demikian, pusat otentifikasi harus siap sedia setiap saat untuk memberikan layanan ketika dihubungi oleh pihak pengguna, hal ini diminimalisasi dalam protokol yang mengizinkan penciptaan sejumlah sesi dalam satu pemanggilan sekaligus. Hal tersebut mengharuskan pusat otentifikasi menyediakan layanan dengan kepercayaan dan ketersediaan tingkat tinggi yang tentunya memakan biaya yang tidak sedikit.

Dengan teknologi digital generasi ketiga yang penyebarannya akan lebih luas, masalah tersebut tentunya akan semakin bertambah berat. Salah satu solusi adalah dengan menggunakan kriptografi kunci publik tidak simetris yang tidak memerlukan server yang siap sedia. Hal tersebut masih sulit untuk diterapkan pada teknologi digital generasi dua karena keterbatasan komputasi alat yang dapat ditangani sekaligus, akan tetapi hal tersebut dimungkinkan pada generasi ketiga. Metode kunci publik tidak simetris pun berpotensi untuk digunakan pada beberapa bidang lain, seperti tanda tangan digital pada transaksi elektronik melalui media komunikasi, sehingga penggunaannya dalam protokol komunikasi nirkabel adalah pilihan yang rasional.

Tujuan dari makalah ini adalah untuk membandingkan berbagai aspek kegunaan protokol kunci publik untuk menjalin komunikasi dan otentifikasi dalam sistem komunikasi nirkabel generasi ketiga. Dalam pembahasannya akan dilakukan pembandingan kelebihan antara protokol perpindahan dan kesepakatan kunci. Selain itu,

akan dilakukan perbandingan dengan protokol yang diajukan dalam sejumlah makalah lain dan mengusulkan protokol yang dianggap sesuai untuk menangani komunikasi nirkabel.

2. Kebutuhan Terhadap Protokol Nirkabel

Proyek ASPeCT [6,10] yang dikembangkan di Eropa telah mengajukan berbagai protokol kunci publik untuk sistem nirkabel 3G yang salah satunya akan dibahas pada sub-bab 3.3. Honr dan Preneel [6] mengajukan enam tujuan protokol otentifikasi antara entitas bergerak dengan jaringan yang tetap.

HP1 Otentifikasi pengguna dan jaringan. Hal ini merupakan kebutuhan umum, karena salah satu kekurangan sistem komunikasi generasi kedua adalah minimnya otentifikasi jaringan. Akan tetapi definisi otentifikasi komponen belum menjadi kesepakatan umum, karena tujuan ini dapat menjadi redundan jika tujuan pembangkitan kunci telah tercapai.

HP2 Kesepakatan antara pengguna dengan jaringan pada sebuah sesi rahasia dengan otentifikasi kunci secara implisit. Hal ini merupakan kebutuhan standar untuk semua protokol pembangkitan kunci, di mana pengguna dan jaringan menyepakati entitas yang boleh mengetahui kunci sesi.

HP3 Konfirmasi kunci dua arah. Ide awal kebutuhan ini adalah untuk meyakinkan bahwa entitas lain memiliki kunci sesi yang sama.

HP4 Jaminan keterbaruan kunci. Meyakinkan bahwa setiap sesi menggunakan kunci yang baru untuk mencegah serangan menggunakan kunci yang disimpan sebelumnya. Akan tetapi, kontrol terhadap mekanisme ini kadang sulit untuk memfasilitasi pilihan kunci sesi salah satu pihak.

HP5 Nirpenyangkalan data pengguna. Hal ini kemungkinan besar dipenuhi dengan penggunaan tanda tangan digital.

HP6 Kerahasiaan data. Kebutuhan ini menekankan bahwa sertifikasi pengguna tidak boleh dikirimkan langsung dalam bentuk tulisan melalui antarmuka radio.

Faktor lain dalam perancangan protokol otentifikasi untuk lingkungan nirkabel adalah keterbatasan kemampuan telepon genggam. Meskipun asumsi bahwa telepon genggam 3G memiliki kemampuan operasi kriptografi kunci publik, namun keterbatasan ukuran, tenaga dan penyimpanan masih perlu dipertimbangkan. Horn dan Preneel [6] menyatakan dalam dasar perancangan bahwa sebisa mungkin kebutuhan komputasi dan penyimpanan disesuaikan dari entitias pengguna dengan jaringan.

2.1. Kesepakatan Kunci atau Perpindahan Kunci

Protokol pembangkitan kunci dapat dibagi menjadi protokol perpindahan kunci dan kesepakatan kunci. Perpindahan kunci terjadi ketika salah satu pihak memilih kunci sesi dan mengirimkannya ke pihak lainnya. Sedangkan pada protokol kesepakatan kunci melibatkan kedua pihak dalam pemilihan kunci sesi. Sebagian besar protokol kesepakatan kunci berbasiskan pada protokol pertukaran kunci Diffie-Hellman[3], yang juga akan menjadi dasar pembahasan pada bagian ini.

Dalam komunikasi nirkabel, kebutuhan terhadap sejumlah komponen kriptografi dalam protokol keamanan jaringan masih diragukan. Misalnya, kebutuhan keterbaruan kunci diragukan jika otentifikasi entitas yang terlibat memberikan jaminan dan tidak menggunakan kunci sesi yang lama. Biasanya kunci masukan dari protokol kesepkatan kunci memiliki komponen acak dan keterlibatan komponen tersebut dalam penghitungan kunci memastikan kunci yang dihasilkan berbeda dari yang sebelumnya. Namun tampaknya makna keterbaruan kunci masih bersinggungan dengan keterbaruan pesan kriptografi yang dilibatkan.

Banyak protokol otentifikasi kunci yang diajukan [1] menggunakan sistem kesepakatan kunci. Penggunaan kesepakatan kunci Diffie-Hellman tampak berlebihan dibandingkan dengan perpindahan kunci, karena hubungan antara pengguna dengan penyedia layanan umumnya tidak simetris. Pengguna layanan mobile pada dasarnya merupakan sebuah entitas privat, sementara pihak penyedia layanan merupakan pihak publik. Terlihat bahwa kebutuhan untuk menyediakan kerahasiaan komunikasi tidak dapat diasumsikan sama untuk kedua jenis entitas yang berbeda.

Jika sebuah skema perpindahan kunci atau kesepakatan kunci berbasiskan fungsi *hash* digunakan, beban komputasi dapat dihemat secara signifikan. Beberapa pendapat yang memungkinkan adalah sebagai berikut.

Pengaturan kunci, kebutuhan HP4 menyatakan bahwa kedua pihak harus turut memutuskan kunci sesi. Karena kedua pihak dapat memberikan kunci sesi kepada pihak yang diinginkan, sehingga basis kebutuhan ini bukanlah kepercayaan, namun kualitas kunci.

Hal tersebut muncul karena komponen mobile dan jaringan tidak dapat melakukan pemilihan kunci sesi, sehingga digunakan fungsi *hash*, yang dapat digunakan pada perpindahan kunci dan kesepakatan kunci. Dengan kata lain, kebutuhan pengaturan kunci dapat dipenuhi oleh semua protokol.

Tidak dibutuhkan enkripsi, karena tingkat kerumitan transfer data keluar dari suatu negara, akan lebih mudah bagi protokol yang tidak mengandung enkripsi secara eksplisit. Konsep Diffie-Hellman hanya membutuhkan tanda tangan, namun protokol tersebut dapat digunakan untuk enkripsi lebih lanjut menggunakan kunci sesi.

Keamanan berkelanjutan, pada konsep Diffie-Hellman, jika kunci privat jangka panjang milik pengguna diketahui pihak lain, hal tersebut tidak memungkinkan untuk kunci publik yang sebelumnya ditemukan oleh penyerang. Meskipun demikian, skenario kesepakatan kunci jangka panjang mustahil digunakan dalam lingkungan mobile.

3. Protokol yang Diajukan

Pada bagian ini, akan dibahas dua protokol yang baru-baru ini diajukan untuk komunikasi nirkabel. Dalam penjelasan, digunakan simbol A untuk pengguna bergerak dan B untuk jaringan. Entitas A dan B memiliki kunci privat x_A dan x_B, dengan kunci publik y_A dan y_B. Semua komputasi menggunakan bilangan bulat modulo bilangan prima p, kecuali dinyatakan berbeda dan terdapat nilai g yang dipilih sehingga logaritma diskrit terhadap g sangatlah sulit. r_A dan r_B adalah nilai acak yang dipilih A dan B, notasi $\{X\}_K$ menunjukkan enkripsi dengan kunci simtris K untuk pesan X.

3.1. Protokol Park

Protokol ini [13] merupakan modifikasi dari protokol yang dirancang Yacobi dan Shmuely [16]. Kunci publik A dan B adalah $y_A = g^{-xA}$ dan $y_B = g^{-xB}$. Dalam protokol asli Yacobi-Schmuely, komputasi dilakukan menggunakan komposit modulo dan bukan bilangan prima p. Protokol pesan adalah sebagai berikut.

1. B → A: $x_B + r_B$
2. A → B: $x_A + r_A$

Kunci sesi adalah $K_{AB} = g^{rArB}$, oleh A penghitungan menjadi $K_{AB} = (g^{xB+rB}y_B)^{rA}$ dan oleh B menjadi $K_{AB} = (g^{xA+rA}y_A)^{rB}$. Berikut adalah perubahan pesan pada protokol Park.

1. B → A: $g^{xB + rB}$
2. A → B: $x_A + r_A$

Kunci sesi yang digunakan $K_{AB} = g^{rArB}$, dengan penghitungan yang sama, akan tetapi A telah memperoleh $g^{xB + rB}$ sehingga usaha komputasi berkurang. Dalam penghitungan di atas terdapat komponen tambahan, yaitu pertukaran sertifikat dan konfirmasi kunci.

Ketidaksimetrisan antara kedua pesan dibuat dengan komputasi alat mobile. Dalam protokol asli Yacobi-Schmuely, kedua pihak harus melakukan dua komputasi eksponensial K_{AB}. Dalam protokol Park, jaringan harus melakukan tiga komputasi eksponensial dan pengguna hanya satu komputasi.

Martin dan Mitchell [10] menemukan sebuah serangan terhadap protokol Park yang memungkinkan penyerang yang memperoleh kunci yang telah digunakan antara A dan B untuk menyamar sebagai B. Serangan tersebut juga berfungsi untuk protokol Yacobi-Shmuely.

Kondisi penyerangan adalah penyerang C memperoleh kunci sesi K_{AB} dari sebuah proses protokol sebelumnya, di mana pesan telah direkam. C memiliki nilai $K_{AB} = g^{rArB}$, x_A+r_A dan g^{xB+rB}. C memulai eksekusi protokol dengan entitas A di mana pesan yang dikirim oleh B adalah balasan dari pesan x_B+r_B yang dikirim oleh B pada eksekusi sebelumnya. Entitas A akan mengirim pesan baru $x_A+x'_A$, akan tetapu dengan mengurangi pesan x_A+x_A yang disimpan, C memperoleh $r_A-r'_A$. Maka penyerang akan menemukan kunci sesi baru $K'_{AB} = g^{r'ArB}$ dengan kalkulasi berikut.

$$K'_{AB} = (g^{x_B+r_B}y_B)^{r'_A-r_A}K_{AB}$$

Perhatikan bahwa komputasi bersifat dua arah, sehingga C dapat menyamar sebagai A atau B. Dalam protokol Park, karena x_B+r_B tidak tersedia bagi penyerang, C hanya dapat menyamar sebagai B.

Kemampuan penyerang untuk memperoleh kunci sesi adalah asumsi dasar dalam analisis protokol, namun ada pendapat yang menyatakan bahwa hal tersebut mustahil dilakukan dalam jaringan telepon genggam. Berikut modifikasi serangan untuk protokol Park.

3.2. Serangan terhadap Protokol Park

Dalam protokol Yacobi-Shmuely x_B+r_B dikirim oleh B sehingga semua pihak dapat memperoleh

g^{rB}. Meskipun demikian, tak ada entitas yang dapat membentuk pesan tersebut, karena hanya B yang mengetahuinya. Dengan modifikasi g^{xB+rB} pada protokol Park, sembarang entitas, misalkan E, dapat membentuk $y_B^{-1}g^{rB}=g^{xB+rB}$ dari y_B dan g^{rB} dengan sembarang nilai acak r_B. Perhatikan bahwa tidak ada tanda pengenal pada g^{xB+rB}.

Dengan perubahan tersebut, tidak terdapat otentifikasi dari B ke A. Sehingga E dapat menjalankan protokol tersebut dengan A tanpa perlu mengetahui kunci privat B.

1. E → A: $g^{xB + rB}$
2. A → E: $x_A + r_A$

Dalam kasus di atas, r_B adalah nilai acak yang dipilih E dan bukan B. E dapat menghitung kunci sesi yang sama dengan B dalam eksekusi normal, karena tidak diperlukan x_B dalam menghitung $K_{AB}=(y_A g^{xA+rA})^{rB}= g^{rArB}$. A percaya bahwa B siap untuk berkomunikasi dengan A dan telah membangkitkan kunci sesi yang sama dengan A. Namun sesungguhnya, penyeranglah yang telah membangkitkannya. Serangan ini tidak mengharuskan E untuk mencoba bermain di antara jaringan dan pengguna.

3.3. Protokol ASPeCT

Protokol ini merupakan kandidat protokol standar UMTS pada 3G untuk otentifikasi dan pembangkitan kunci berdasarkan kriptografi asimetri. Selain itu protokol ini diperuntukkan bagi pengguna untuk nilai tambah penyedia layanan (VASP). Entitas A mewakili pengguna dan B mewakili jaringan, dengan CA adalah pemberi sertifikasi. Kunci publik A dan B adalah $y_A=g^{xA}$ dan $y_B=g^{xB}$.

h_1, h_2, h_3 adalah fungsi *hash*. $Sig_A\{X\}$ adalah transformasi tanda tangan A pada pesan X. *ACert* adalah sertifikat A yang mengandung informasi varifikasi tanda tangan publik A. *BCert* adalah sertifikat B yang mengandung kunci publik B g^B. *chd* adalah data yang ditambahkan. *Pay* adalah data pembayaran. T_B adalah komponen waktu yang diberikan B.

1. A → B: g^{rA}, *CA*
2. B → A: r_B , $h_2(K_{AB},r_B,B)$,*chd*, T_B, *BCert)*
3. A→B:$\{Sig_A(h_3(g^{rA},g^b,r_B,B,chd,TS,pay)),Acert,pay\}_{Kab}$

Kunci sesi dihitung A sebagai $K_{AB}=h_1(r_B,y_B^{rA})$ dan oleh B sebagai $K_{AB}=h_1(r_B,(g^{rA})^{xB})$.

Protokol ini telah dimodifikasi beberapa kali, perubahan terbaru adalah penambahan identitas B dalam pesan ketiga. Penambahan tersebut merupakan aplikasi rancangan kriptografi. Meskipun hubungan A dan B digolongkan ke dalam pengguna dan penyedia layanan.

Penambahan r_B dalam pesan kedua tidak memiliki dampak langsung dalam pencapaian tujuan, melainkan untuk menambahkan catatan waktu dan mencegah serangan dari faktor tersebut. Hal lain yang menarik adalah identitas B dalam pesakn kedua. Beberapa makalah [6] menyatakan tujuannya adalah untuk mencegah serangan dengan pertukaran sumber yang dimungkinkan hanya dengan pendaftaran B secara tak terotentifikasi dengan CA. Hal ini penting jika kunci publik akan digunakan untuk tujuan lain, seperti aplikasi transaksi elektronik.

3.4. Kelemahan Protokol ASPeCT

Kelemahan yang paling diperbincangkan dari protokol ini adalah waktu tunda dalam identifikasi entitas A hingga titik pesan ketiga. Alasannya adalah untuk meyakinkan kerahasiaan pengguna dan memenuhi kebutuhan HP6. Waktu tunda tersebut, ternyata bukan akibat dari kerahasiaan pengguna, namun akibat tipe otentifikasi yang digunakan. Biasanya, pesan pertama mengandung identitas A. Dalam otentifikasi yang digunakan, tidak ada pihak yang dapat menggunakan entitas tambahan untuk melakukan operasi kriptografi selain kunci privat masing-masing.

Skenario serangan yang mungkin adalah dengan memotong pesan ketiga, mencegah B dari menerima pesan. Tentunya, penyerang tak dapat memperoleh kunci sesi. Sehingga meskipun A telah telah menandatangani detil transaksi, B tidak akan mengetahui bahwa A telah melakukannya. Serangan ini cocok digunakan antar para pesaing penyedia layanan VASP. Meskipun serangan ini dapat dilakukan pada semua protokol, pada kasus ini B tidak dapat mengetahui identitas A hingga pesan ketiga.

Kemungkinan serangan tersebut adalah akibat kurangnya media untuk memastikan bahwa bukan hanya kunci yang digunakan adalah benar, namun juga kunci tersebut terasosiasi dengan pihak yang sesuai. Komponen tersebut dapat ditambahkan pada daftar kebutuhan dalam setiap protokol kesepakatan. Perbandingan yang bermanfaat dapat dibuat dengan serangan ini dan serangan Lowe[9] pada protokol STS[4]. Serangan tersebut didasarkan pada pemikiran bahwa A mengira

sedang berkomunikasi dengan A, akan tetapi B tidak pernah mengenal A.

4. Protokol yang Diajukan

Melalui pertimbangan kebutuhan entitas mobile dan kelemahan dari protokol yang dipublikasikan, berikut adalah ide untuk protokol otentifikasi dan pembangkitan kunci dalam dua versi, yaitu menggunakan perpindahan kunci dan kesepakatan kunci.

Notasi untuk menjelaskan protokol adalah sama dengan yang digunakan sebelumnya, dengan tambahan area COUNT. Penambahan area tersebut bertujuan untuk mendeteksi penipuan identitas pengguna. Penggunaan area tambahan tersebut dijelaskan pada [14] dan turut membentuk pendekatan keamanan komunikasi nirkabel. Notasi *En* c_B{X} menyatakan enkripsi X menggunakan kunci publik B.

1. A → B: *En* $c_B\{A,K_{AB},COUNT\}$
2. B → A: $\{COUNT, r_B\}_{Kab}$
3. A → B: $Sig_A\{B,h(COUNT,K_{AB},r_B)\}$

Dalam contoh kedua, baik A dan B turut menentukan kunci sesi, yang dihitung dengan $K_{AB} = h(r_A,r_B)$ untuk sebuah kunci *hash h* yang sesuai.

1. A → B: *En* $c_B\{A,r_A,COUNT\}$
2. B → A: $rB,\{COUNT, r_A\}_{Kab}$
3. A → B: $Sig_A\{B,h(COUNT,r_B,K_{AB})\}$

Diasumsikan bahwa A dan B memiliki akses ke kunci publik masing-masing. Sehingga ketika A mengambil kunci publik dari jaringan, dia dapat menerima kunci dari saluran sistem tersiar dalam jaringan. B dapat memperoleh kunci publik dari pengguna melalui data sertifikat A yang dimasukkan bersama informasi terenkripsi dalam pesan pertama.

Pesan kedua menyediakan konfirmasi kunci untuk A. Pesan ketiga menyediakan konfirmasi kunci dan keterbaruan untuk B. Pesan ketiga juga menyediakan fitur nirpenyangkalan untuk aplikasi transaksi elektronik. Perhatikan bahwa pesan pertama dapat dihitung sebelum terkoneksi ke jaringan oleh entitas mobile. Identitas A disimpan dalam pesan pertama yang dienkripsi menggunakan kunci publik B untuk kerahasiaan pengguna. Perhatikan bahwa kelemahan protokol ASPeCT tidak ditemukan pada protokol ini. Lebih jauh lagi, penggunaan identitas A dalam pesan pertama adalah langkah pencegahan serangan antara jaringan dan pengguna.

Martin dan Mitchell [10] telah menunjukkan bahwa sejumlah tanda tangan dapat membocorkan informasi identitas pengirimnya. Hal tersebut terjadi jika prosedur verifikasi dapat mengungkap struktur pengulangan dalam tanda tangan dan tidak membutuhkan pesan bertandatangan. Pada protokol ini, digunakan tanda tangan tipe ElGamal atau Schnorr [15]. Hal tersebut menutup kemungkinan serangan yang dijelaskan sebelumnya, juga memberikan keuntungan bahwa hampir semua komputasi dapat dilakukan tanpa perlu terhubung dengan jaringan. Tipe yang lebih cocok adalah salah satu varian elips dari tanda tangan ElGamal yang sedang distandarisasi [7]. Hal tersebut memberikan komputasi yang lebih efisien dan penyimpanan yang lebih besar dan berguna untuk telepon genggam.

Jika dibandingkan dengan protokol ASPeCT, terdapat sejumlah fitur serupa. Dalam kedua protokol, meskpun pihak mobile diharuskan melakukan operasi kunci publik, sebagian besar dapat dilakukan tanpa perlu terhubung dengan jaringan. Sehingga dapat diasumsikan bahwa identitas B diketahui oleh A. Hal tersebut berarti dalam protokol ASPeCT, nilai g^{rAxB}, yang digunakan dalam penghitungan K_{AB}, dapat dilakukan oleh A tanpa perlu terhubung dengan jaringan. Hal yang sama berlaku pada pesan pertama di protokol yang diajukan. Sehingga tersisa fungsi *hash*, enkripsi simetri dan pembangkitan tanda tangan yang dilakukan ketika terhubung dengan jaringan. Bahkan, pemilihan algoritma yang sesuai memungkinkan sebagian besar usaha pembangkitan tanda tangan dilakukan tanpa perlu terhubung dengan jaringan.

Satu-satunya kerugian yang ditemukan adalah kurangnya kerahasiaan jangka panjang, akan tetapi hal ini juga menjadi kelemahan dari protokol ASPeCT, karena kesepakatan kunci jangka panjang pada jaringan memungkinkan kunci sesi dikembalikan dengan menjalankan protokol menggunakan data yang telah direkam.

5. Kesimpulan

Setelah mempertimbangkan kebutuhan protokol pembangkitan kunci dan otentifikasi, dilakukan analisis sejumlah protokol yang diajukan baru-baru ini, dengan beberapa kekurangannya. Selain itu, juga dilakukan analisis terhadap protokol persetujuan kunci menggunakan metode Diffie-Hellman dan terbukti melakukan operasi yang sia-sia dan mahal secara komputasi.

Dari langkah tersebut, diajukan sebuah protokol yang berusaha menghindari kekurangan yang ditemui. Namun belum terdapat bukti formal dan analisis keamanan untuk protokol yang diajukan, sehingga saran dan masukan sangat diharapkan untuk menguatkan protokol tersebut.

REFERENSI

[1] C. Boyd dan A. Mathuria, "*Key Establishment Protocols for Secure Mobile Communications: A Selective Survey*", Information Security and Privacy, LCNS 1438, Springer-Verlag, 1998, hlm.344-355.

[2] D. Denning and G. Sacco, "*Timestamps in Key Distribution Protocols*", Communications of the ACM, 34, 1981 hlm.533-536

[3] W.Di e and M. Hellman, "*New Directions in Cryptography*", IEEE Transaction on Information Theory, 22, 1976, hlm.644-654

[4] 4. W. Diffie, P. van Oorshot and M. Wiener, "*Authentication and Authenticated Key Exchanges*", Designs, Codes and Cryptography, 2, 1992, hlm.107-125.

[5] D. Gollman, "*What do we Mean by Entity Authentication*", IEEE Symposium on Security and Privacy, hlm.46-54, 1996.

[6] G. Horn and B.Preneel, "*Authentication and Payment in Future Mobile Systems*", Proceedings of ESORICS'98, Springer-Verlag, 1998.

[7] IEEE P1363 Standard Speci cations for Public Key Cryptography, Draft Version, September 1998.

[8] ISO-IEC, DIS 11770-3 Key Management - Part 3: Mechanisms using Asymmetric Techniques, 1996.

[9] G. Lowe, "*Some New Attacks upon Security Protocols*", 9th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 1996, hlm.162-169.

[10] Keith Martin and Chris Mitchell, "*Evaluation of Authentication Protocols for Mobile Environment Value-added Services*", Draft, 1998.

[11] A. Mehrota, GSM System Engineering, Artech House, 1997.

[12] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Ahlmlied Cryptography, CRC Press, 1997.

[13] C.-S. Park, "*On Certificate-Based Security Protocols for Wireless Mobile Communication Systems*", IEEE Network, September/October 1997, hlm.50-55.

[14] D.-G. Park, M.-N. Oh and M. Looi, "*A Fraud Detection Method and Its Ahlmlication to Third Generation Wireless Systems*", Proceedings of Globecom'98.

[15] C. Schnorr, "*E cient Signature Generation by Smart Cards*", Journal of Cryptology, 4, 1991, hlm.161-174.

[16] Y. Yacobi and Z. Shmuely, "*On Key Distribution Systems*", Advances in Cryptology - Crypto'89, Springer-Verlag, hlm.344-355.

[17] Y. Yacobi, "*A Key Distribution "Paradox*", Advances in Cryptology CRYPTO'90, Springer-Verlag 1991, hlm.268-273.