KERENTANAN KEAMANAN DI WIMAX MOBILE DAN SOLUSINYA

Helmi Kurniawan[1], Reza Pulungan[2]

[1]Program Studi Teknik Informatika, STMIK Potensi Utama, Medan
[2]Jurusan Ilmu Komputer dan Elektronika, Universitas Gadjah Mada, Yogyakarta
[1]STMIK Potensi Utama, Jl.K.L.Yos Sudarso Km.6,5 No.3-A Tj.Mulia Medan
[2]Universitas Gadjah Mada, Bulaksumur, Yogyakarta 55281
[1]helmikk12@gmail.com, [2]pulungan@ugm.ac.id

Abstrak

Teknologi WIMAX memiliki kerentanan terhadap faktor interferensi yang diakibatkan oleh beberapa faktor (cuaca/iklim, gelombang radio lain, dan noise-noise yang lain). Hal ini menjadi tantangan bagi kita untuk mengantisipasi kendala ini dengan mengembangkan teknologi wireless yang bebas interferensi. Makalah ini menunjukkan kerentanan keamanan yang berbeda ditemukan di IEEE 802.16e dan memberikan solusi yang mungkin untuk menghilangkannya. Kerentanan ini adalah kemungkinan untuk memalsukan pesan kunci dalam operasi Multi dan Broadcast, beberapa pesan yang tidak berkepentingan yang rentan terhadap pemalsuan dan manajemen komunikasi terenkripsi yang mengungkapkan pentingnya manajemen informasi.

Kata kunci**:** IEEE 802.16e security, multi- and broadcast service, shared key vulnerability, hash chaining solution

1. Pengantar IEEE 802.16e

1.1 Pengantar Umum

Perkembangan IEEE 802.16 dimulai oleh IEEE pada tahun 2001. Setelah itu telah direvisi beberapa kali dan berakhir pada akhir standar IEEE 802.16-2004 yang sesuai dengan revisi D dan sering disebut Fixed WiMAX [1]. Hal ini mendefinisikan Broadband Wireless Metropolitan akses untuk digunakan stasioner dan nomaden. Ini berarti perangkat akhirnya tidak dapat bergerak di antara base station (BS) tetapi mereka bisa masuk jaringan pada lokasi yang berbeda.

Spesifikasi ini diperpanjang oleh pengembangan IEEE 802.16e yang mendukung mobilitas sehingga mobile station (MS) dapat serah terima antara BS saat berkomunikasi. IEEE 802.16e sering disebut Mobile WiMAX [2] dan merupakan perubahan terhadap standar IEEE 802.16-2004. Layanan Komersial Mobile WiMAX yang sudah direncanakan untuk beberapa negara.

Pada link layer Mobile WiMAX memperkenalkan fitur baru seperti jenis penyerahan yang berbeda, metode hemat daya dan multi-dan dukungan broadcast. Selanjutnya IEEE 802.16e menghilangkan sebagian besar kerentanan keamanan ditemukan di pendahulunya [3]. Menggunakan otentikasi berbasis saling EAP, berbagai algoritma enkripsi yang kuat, nonces dan nomor paket untuk melindungi terhadap serangan replay dan mengurangi daya tahan key. Pertama-tama beberapa bagian dari fungsi Mobile WiMAX diperkenalkan. Setelah itu kerentanan keamanan dan solusi yang mungkin berbeda untuk memecahkannya.

1.2 Prosedur Entri

Awal untuk masuk jaringan, MS harus dilanjutkan melalui beberapa langkah. Pertama harus mencari pesan peta downlink dari BS yang ditampilkan secara berkala. Format ini berisi informasi tentang sambungan mulai awal identifier (CID), yang berhubungan dengan timeslot di mana proses awal mulai dapat dilakukan. Akses ke timeslot ini umum digunakan didefinisikan sebagai CSMA. MS kemudian meningkatkan daya transmisi dengan masing-masing permintaan mulai mengirimkan pada awal mulai slot sampai menerima tanggapan dari BS. Respon ini mencakup mulai penyesuaian dan CIDs manajemen dasar dan primer yang cadangan interval waktu tertentu untuk MS mengirim dan menerima pesan manajemen. Setelah awal mulai selesai kemampuan dasar untuk sambungan dinegosiasikan.

Maka proses otentikasi berikut. IEEE 802.16e menyediakan RSA-otentikasi atau otentikasi EAP-based sederhana. Otentikasi EAP mencakup otentikasi berbasis lapisan yang lebih tinggi dan karenanya dapat dianggap sebagai metode yang paling aman. Setelah proses otentikasi MS dan BS telah menyiapkan sebuah kunci otorisasi umum (AK). Kemudian kunci enkripsi kunci (KEK) adalah berasal dari AK yang aman digunakan untuk mentransfer kunci lebih lanjut. Juga kunci untuk otentikasi pesan dalam downlink-up dan berasal dari AK.

Setelah ini, TEK 3-way-tukar untuk setiap sambungan data dijalankan. Ini berarti pertukaran MS dan BS tombol yang akhirnya digunakan untuk lalu lintas enkripsi data. Dengan ini setiap pesan adalah integritas dilindungi melalui MAC mencerna dan lalu lintas kunci enkripsi dialihkan (TEK) dienkripsi oleh KEK tersebut. Selanjutnya setiap MS harus mendaftar di BS dan diizinkan untuk mengirim data ke jaringan. Untuk MSS mengelola proses pendaftaran tambahan membuat sebuah CID

manajemen sekunder yang diperlukan untuk mengelolanya.

1.3 Manajemen Kunci

Dengan cara 3-TEK Bursa diproses pada awal masuk jaringan, MS membuat sebuah asosiasi keamanan (SA) untuk setiap komunikasi data yang ingin membangun. Seperti sebuah asosiasi keamanan mengelola kunci untuk enkripsi data (Teks), daya tahan dan parameter keamanan lainnya yang berhubungan dengan hubungan ini. Ini juga termasuk mesin TEK kondisi yang memiliki tugas untuk secara berkala memperbarui bahan masukkan ketika masa dari TEK akan kadaluarsa.

Untuk meminta bahan key yang baru mesin kondisi mengirimkan permintaan key untuk BS yang merespon dengan tanggapan key termasuk TEK baru. TEK ini ditransfer dienkripsi dengan kunci enkripsi kunci (KEK) yang berasal dari AK dan global digunakan untuk mendekripsi kunci yang diterima dari semua DS.

Gangguan komunikasi Untuk mencegah setiap SA secara bersamaan memegang dua TEKS. Ketika satu TEK berakhir yang kedua digunakan untuk enkripsi lalu lintas dan yang baru diminta.

1.4 Optional Sleep Mode

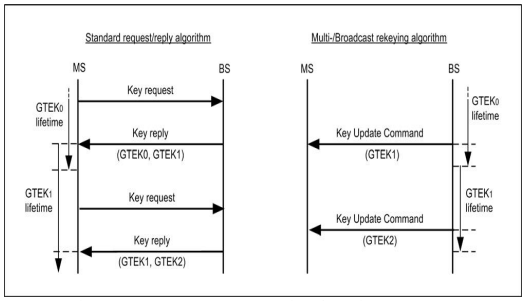
Untuk menyimpan stasiun kapasitas baterai dan mengurangi beban pada saluran, modus sleep opsional didefinisikan di Mobile WiMAX. Hal ini memungkinkan MS untuk absen dari BS melayani untuk jangka waktu tertentu dan listrik dapat menurunkan pemancar nya. Oleh karena itu IEEE 802.16e menetapkan tiga set berbeda kelas penghematan daya. Layanan dengan sifat permintaan umum harus dipetakan ke set yang sama dari kelas hemat daya. Setiap kelas hemat daya mendefinisikan periode waktu ketika MS harus dalam keadaan aktif, mendengarkan untuk transmisi, dan periode dimana itu diperbolehkan untuk mengubah ke modus sleep. Jika MS memiliki kekuatan aktif penghematan kelas yang berbeda, overlay periode sleep diatur di kelas semua penghematan daya mendefinisikan jendela sleep akhir. Oleh karena MS hanya dapat berubah ke modus sleep ketika semua daya yang digunakan hemat kelas kali ini mendefinisikan sebagai waktu sleep. Jika setidaknya satu koneksi bukan milik kelas ke penghematan daya, MS tidak dapat mengubah ke modus sleep.

Ketika sebuah MS sedang sleep itu tidak berkomunikasi dengan BS dan dapat mematikan pemancarnya. Namun MS mampu menjalankan semua proses lain seperti misalnya mulai atau pengukuran tetangga yang tidak memerlukan komunikasi dengan melayani BS. Ketika BS ditakdirkan untuk menerima data MS sleep, data ini adalah buffered dan MS terbangun dengan pesan Indikasi Traffic ditampilkan.

1.5 Multi-and Broadcast Service (MBS)

IEEE 802.16e juga memperkenalkan layanan untuk Multicast dan komunikasi Broadcast. Hal ini memungkinkan BS untuk mendistribusikan data secara bersamaan untuk beberapa MSS. Untuk mengamankan komunikasi siaran IEEE 802.16e menggunakan kunci enkripsi lalu lintas kelompok umum (GTEK) untuk lalu lintas en-/decryption. Setiap anggota kelompok harus mengetahui kunci ini. Untuk berbagi GTEK antara MS dan BS dua algoritma seperti yang ditunjukkan pada Gambar 1 yang digunakan: Permintaan kunci wajib / reply mekanisme dan algoritma Multi-dan Broadcast opsional rekeying (MBRA). Dalam permintaan standar / mekanisme balasan MS untuk mengelola update GTEK dengan sendirinya. Ini berarti harus meminta bahan keying baru jika kunci saat ini akan kadaluarsa. Seperti permintaan kunci memicu respons kunci unicast dari BS yang mencakup kunci baru. Untuk menjamin komunikasi berjalan MS secara bersamaan memegang dua kunci mirip dengan manajemen TEK kunci yang dijelaskan di atas.

Sebuah alternatif pilihan untuk mendistribusikan bahan keying adalah rekeying Multi-dan Broadcast algoritma (MBRA). Berikut tombol dikelola oleh BS. Jika masa kunci akan berakhir, siaran BS satu kunci pesan Update Perintah untuk semua MSS. Ini menghemat banyak bandwidth karena GTEKs yang sangat sering diperbarui. Untuk mengenkripsi GTEK ditampilkan, kunci enkripsi kelompok kunci (GKEK) diperlukan (tidak ditampilkan pada Gambar 1). GKEK ini di-update tidak terlalu sering. Hal ini juga didistribusikan dengan pesan Update Key Command, tapi dengan cara unicast dienkripsi oleh KEK MS-terkait. Jika MS belum menerima kunci baru setelah waktu tertentu, itu permintaan bahan keying sesuai dengan menjawab permintaan standar / mekanisme. Hal ini juga dilakukan jika nilai otentikasi dari pesan Update Key Perintah tidak valid.



Gambar 1. Permintaan standar / mekanisme yg dibandingkan dengan MBRA

Sumber: Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol.

1.6 Analisis Keamanan WiMAX

Keamanan WiMAX Tetap dianalisis dalam beberapa makalah. Terutama di kerentanan keamanan [3] banyak diuraikan. Dengan perubahan publikasi WiMAX Mobile, sebagian besar dari kerentanan tersebut diselesaikan. Keamanan IEEE 802.16e hanya dianalisis oleh beberapa makalah. [5] Memeriksa pertukaran 3-way TEK dan proses otorisasi dan tidak dapat menemukan kebocoran keamanan. Protokol manajemen kunci juga [6] dianalisis menganalisis protokol menggunakan perangkat lunak dan tidak menemukan masalah apapun.

Layanan dan multi siaran diperiksa [7] dengan menganalisis protokol menggunakan alat. Ini menemukan bahwa keamanan MBS didasarkan pada beberapa parameter yang harus diterapkan dengan benar untuk perlindungan lengkap. Hal ini juga menunjukkan bahwa interoperation dengan protokol lain bisa menjadi masalah keamanan jika protokol ini memiliki karakteristik keamanan yang lebih rendah.

2. Kerentanan dalam IEEE 802.16e

Bagian ini menjelaskan kerentanan ditemukan di Mobile WiMAX dengan analisisnya. Kerentanan ini adalah:

- Pesan yang tidak berkepentingan Mobile WiMAX meliputi beberapa pesan yang tidak berkepentingan. Pemalsuan mereka dapat membatasi atau bahkan mengganggu komunikasi antara mobile station dan base station.
- Tak terenkripsi komunikasi Manajemen komunikasi yang lengkap antara manajemen mobile station dan base station tidak terenkripsi. Jika musuh mendengarkan lalu lintas, ia dapat mengumpulkan banyak informasi tentang kedua kasus.
- Dibagi kunci dalam layanan-multi dan ditampilkan Untuk lalu lintas enkripsi simetris, multi-dan layanan siaran Mobile WiMAX keying dengan semua anggota kelompok. Ini memperkenalkan kerentanan yang anggota kelompok bisa membina pesan atau bahkan menyebarkan bahan lalu lintas keying sendiri, sehingga mengendalikan multi dan isi siaran.

2.1 Pesan Terauthentikasi

Sebagian besar pesan manajemen didefinisikan dalam IEEE 802.16e adalah integritas dilindungi. Hal ini dilakukan dengan kode pesan otentikasi berbasis hash (HMAC) [8] atau alternatif dengan kode sandi otentikasi berbasis pesan (CMAC) [9]. Namun, beberapa pesan yang tidak termasuk dalam setiap mekanisme otentikasi. Ini memperkenalkan beberapa kerentanan.

Pertama harus disebutkan bahwa beberapa pesan manajemen dikirim melalui koneksi manajemen siaran. Otentikasi pesan manajemen ditampilkan sulit karena tidak ada kunci yang sama untuk menghasilkan mencerna pesan. Selanjutnya sebuah kunci yang sama tidak akan sepenuhnya melindungi integritas dari pesan sebagai stasiun bergerak berbagi tanda bisa membina pesan-pesan ini dan menghasilkan digit otentikasi yang valid.

2.1.1 MOB_TRF-IND

Salah satu pesan manajemen tersiar dan terauthentikasi adalah pesan *Traffic Indication* (MOB_TRF-IND). Pesan ini digunakan oleh BS untuk menunjukkan ke MS sleep bahwa ada lalu lintas yg diperuntukkan untuk itu. Oleh MS terbangun dari modus sleep. Sebuah sleep unik ID ditugaskan untuk setiap MS di kisaran stasiun base. Ini sleep ID adalah nilai 10 bit 1023 MSS yang berbeda. Untuk mempercepat pemrosesan pesan, pesan indikasi menggabungkan lalu lintas 32 ID Sleep untuk satu Sleep Group ID. Dengan demikian terdapat 32 Sleep kelompok ID berisi 32 Sleep ID masing-masing. Jika BS sekarang menerima lalu lintas untuk MS Sleep, ID grup untuk kelompok Sleep MSS ID diatur ke benar.

Ketika menerima pesan ini, setiap MS dalam kelompok akan memeriksa apakah lalu lintas yang ditujukan kepadanya memverifikasi bitmap indikasi lalu lintas. Nilai ini adalah 32 bit yang ditambahkan untuk setiap kelompok ID Sleep dan berisi sedikit untuk setiap MS individu dalam kelompok itu. Jika bit terkait dalam bitmap indikasi lalu lintas diset, MS masing-masing bangun dan dapat menerima lalu lintas. Semua MSS lainnya dapat melanjutkan Sleep setelah memverifikasi bahwa Sleep ID grup indikasi sedikit kelompok mereka diatur ke false.

Seorang musuh bisa menghasilkan pesan ini yang sering bangun MSS dan stres baterai mereka. Jika semua bit dalam kelompok bitmap ID Sleep indikasi dan semua bitmap indikasi lalu lintas di pesan ini diatur ke benar, setiap MSS dicapai dalam mode Sleep dipaksa untuk bangun.

2.1.2 MOB_NBR-ADV

Ads neighbor messages (MOB_NBR-ADV) juga tidak valid. BS melayani mengirimkan pesan ini untuk mengumumkan karakteristik BS sekitarnya kepada MSS mencari kemungkinan serah terima. Sebuah musuh mampu menahan BSS individu dengan menghilangkan informasi tentang keberadaan mereka ketika ia memasulkan pesan ini. Hal ini untuk mencegah MSS untuk diserahkan pada BSS yang mungkin memiliki karakteristik yang lebih baik sebagai BS mereka melayani. Dia juga dapat mendistribusikan data salah tentang BSS sekitar atau mengumumkan ada non BSS.

2.1.3. FPC

Fast Power Control (FPC) pesan juga ditayangkan tidak termasuk dalam setiap mekanisme otentikasi. FPC Pesan dikirim oleh BS untuk satu atau beberapa MS untuk menyesuaikan kekuatan

transmisinya. Dengan menyalahgunakan pesan ini adalah mungkin untuk mengurangi daya transmisi dari semua MSS dapat dicapai untuk minimum sehingga menjadi rendahnya untuk dikenal oleh BS.

Dengan demikian, penyesuaian daya rekursif diperlukan untuk MS sampai daya transmisi cukup kuat untuk mencapai BS lagi. Karena CSMA, yang diakumulasikan pengaturan daya tiba-tiba memicu pesan mengakibatkan permintaan bandwidth uplink banyak. Hal ini menyebabkan collisions dalam permintaan contention slot uplink bandwidth dari MSS dan penundaan waktu sampai setiap MS sekali lagi memiliki kekuatan transmisi yang benar dan dapat berkomunikasi dengan BS.

Penyalahgunaan pesan lain ini adalah untuk mengatur kekuatan pemancar dari semua MSS semaksimal mungkin dengan maksud untuk masing-masing tegangan baterainya.

2.1.4 MSC-REQ

Pesan terauthentikasi unicast adalah *Multicast Assignment Request* (MSC-REQ). Saat mengirim pesan ini BS dapat menghapus MS dari sebuah multicast polling kelompok. Sebuah MS yang menerima pesan seperti menghapus menghapus diri dari polling kelompok dan kemudian mengirim respon kembali ke BS. Pembicaraan ini dilakukan dengan menggunakan koneksi manajemen utama antara BS dan MS.

Sebuah polling kelompok adalah sekelompok MS yang bisa mendapatkan bandwidth dari BS melalui mekanisme polling. Oleh karena itu BS mengalokasikan kesempatan uplink transmisi untuk setiap MS dalam polling kelompok. Kemudian MSS dapat meminta bandwidth uplink menggunakan kesempatan ini transmisi.

Karena tidak ada otentikasi untuk pesan ini penyerang dapat dengan mudah menghapus MSS dari polling kelompok. Jika MS akan dihapus dari polling kelompok, telah menggunakan pendapat wajib algoritma alokasi berbasis bandwidth yang mengakibatkan keterlambatan uplink yang lebih besar.

2.1.5 DBPC-REQ

Pesan *Downlink Burst Profile Change Request* (DBPC-REQ) adalah pesan unicast lebih lanjut tanpa perlindungan integritas. Ketika jarak antara BS dan MS bervariasi atau karakteristik komunikasi berubah karena alasan lain, BS mengirimkan pesan ini untuk mengubah profil untuk MSS sangat penuh yang lebih kuat atau yang lebih satu efektif. Niat dalam menyalahgunakan pesan ini dapat untuk sementara waktu istirahat komunikasi antara MS dan BS dengan mengubah profil MSS sangat penuh sehingga tidak mungkin bagi MS untuk demodulasi data yang diterima dari BS.

2.1.6. PMC-REQ

Setiap MS bekerja baik pada *mode loop power control* terbuka atau tertutup. *power control mode* dari suatu MS dapat diubah oleh MS sendiri dengan mengirimkan *Power Control Mode Change Request* (PMC_REQ) untuk BS. BS lalu menjawab dengan *Power Control Mode Change Request* (PMC_RSP). Pesan ini juga dapat dikirim oleh BS dengan cara yang tidak diminta untuk mengubah *Power Control Mode* MSS. Ini juga termasuk nilai daya penyesuaian yang harus dibentuk oleh MS. Pesan PMC_REQ dapat digunakan oleh musuh untuk meminta perubahan *Power Control Mode* MSS. Pesan diterima seolah-olah berasal dari MS.

Kerentanan lain adalah pemalsuan dari *Power Control Mode Change Request* (PMC_RSP) pesan yang dikirim dari BS. Dengan pesan ini musuh secara langsung dapat mengubah *Power Control Mode* dari MS dan juga menyesuaikan transmisi tenaga listrik dengan maksud untuk mengganggu komunikasi.

2.1.7 MOB_ASC-REP

Hasil laporan asosiasi (MOB_ASC-REP) adalah pesan lain tidak sah. Ketika MS dan BS tersebut mempertahankan asosiasi level 2, BS tidak langsung harus menjawab Permintaan Mulai. Sebaliknya itu adalah mengirimkan Tanggapan Mulai dari backbone ke BS menyajikan dari MS meminta. BS menyajikan mengumpulkan semua Respon Mulai dari BSS sekitarnya dan menggabungkan mereka untuk satu pesan laporan asosiasi. Pesan dikumpulkan ini diteruskan ke MS melalui koneksi manajemen dasar.

Pesan respon berkisar antara dirinya sendiri adalah integritas yang dilindungi pada sebagian besar kasus tetapi pesan laporan asosiasi tidak pernah. Seorang musuh bisa mengubah data respon sewenang-wenang dalam pesan seperti penyesuaian waktu atau kekuasaan. Selanjutnya pesan berisi prediksi pelayanan BS yang mengiklankan layanan yang BS dapat menawarkan ke MS. Di sini musuh bisa memalsukan pesan dengan cara yang kelihatannya seperti tidak ada layanan yang tersedia untuk permintaan MS.

2.1.8 *Ranging Request* (Mulai Permintaan)

Untuk *Ranging Request* (RNG-REQ) pesan standar tidak secara eksplisit menetapkan waktu otentikasi yang mencerna akan ditambahkan Di sini harus dinyatakan bahwa pesan ini harus selalu dilindungi oleh digest ketika Authentication Key (AK) tersedia. Untuk masuk jaringan awal tidak ada kunci otentikasi yang tersedia tetapi dalam kasus lain kebanyakan AK ada dan pesan dapat dilindungi. Selain itu ada non-pesan otentik tetapi pemalsuan informasi dibawa mereka dapat dianggap sebagai kurang berbahaya bagi operabilitas dari protokol.

2.2 Manajemen Komunikasi Unencrypted

Topik pesan yang tidak terenkripsi telah dibahas dalam beberapa makalah untuk WiMAX. Dalam Mobile WiMAX pesan manajemen masih dikirim jelas. Risiko konsekuensial harus diuraikan dalam bagian ini. Ketika sebuah MS melakukan entri awal jaringan, melakukan negosiasi parameter komunikasi dan pengaturan dengan BS. Di sini banyak informasi yang dipertukarkan seperti parameter negosiasi pengamanan, pengaturan konfigurasi, parameter mobilitas, pengaturan daya, informasi vendor, MSS dll. Saat ini kemampuan melakukan pertukaran pesan manajemen yang lengkap dalam proses entri jaringan tidak terenkripsi dan informasi di atas dapat diakses hanya dengan mendengarkan di channel tersebut.

Setelah masuk jaringan awal, komunikasi manajemen selama koneksi manajemen dasar dan utama tetap tidak terenkripsi. Karena sebagian besar manajemen pesan dikirim pada koneksi ini, hampir semua informasi manajemen dipertukarkan antara MS dan BS dapat diakses oleh musuh yang mendengarkan. Pesan-satunya yang transfer dienkripsi adalah pesan kunci. Tapi dalam kasus ini hanya kunci dialihkan terenkripsi, semua informasi lainnya masih dikirim jelas.

Musuh mengumpulkan informasi manajemen dapat membuat profil rinci tentang MSS termasuk kemampuan perangkat, pengaturan keamanan, asosiasi dengan stasiun base dan semua informasi lainnya yang dijelaskan di atas. Menggunakan data yang ditawarkan dalam laporan daya, pendaftaran, mulai dan serah terima pesan, musuh yang mendengarkan dapat menentukan pergerakan dan posisi perkiraan dari MS juga. Pemantauan alamat MAC dikirim mulai dalam pesan atau mengungkapkan pendaftaran pemetaan CID dan alamat MAC, sehingga memungkinkan untuk secara jelas berhubungan informasi yang dikumpulkan untuk pengguna peralatan.

Shared Kunci pada Layanan Multi dan Broadcast

Layanan Multi dan Broadcast menawarkan kemungkinan untuk mendistribusikan data ke MS berganda dengan satu pesan tunggal. Hal ini menghemat biaya dan bandwidth. Pesan ditampilkan di 802.16e IEEE akan dienkripsi dengan kunci simetris bersama. Setiap anggota dalam kelompok memiliki kunci dan dengan demikian dapat mendekripsi lalu lintas. Juga pesan otentikasi didasarkan pada key yang bersama sama. Algoritma ini berisi kerentanan bahwa setiap anggota kelompok, selain pesan dikirimkan decrypting dan verifikasi, juga dapat mengenkripsi dan mengesahkan pesan seolah-olah mereka berasal dari 'real' BS.

Aspek lain yang jauh lebih bermasalah adalah distribusi dari kunci enkripsi lalu lintas (GTEKs) ketika Multi opsional-dan Broadcast Rekeying Algoritma (MBRA) digunakan. Untuk mentransfer GTEK ke semua anggota kelompok itu ditampilkan tapi dienkripsi dengan kunci enkripsi kunci (GKEK). Karena penyiaran, yang GKEK juga harus menjadi kunci bersama dan setiap anggota kelompok tahu itu. Jadi anggota kelompok musuh dapat menggunakannya untuk menghasilkan valid terenkripsi dan dikonfirmasi pesan perintah update GTEK kunci dan mendistribusikan GTEK sendiri.

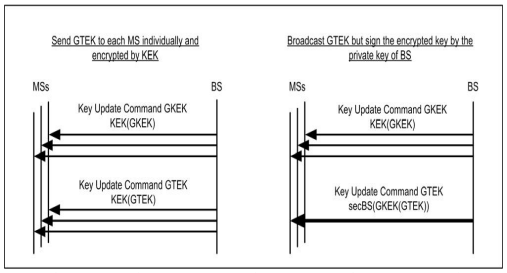
Setiap anggota kelompok akan menetapkan kunci musuh sebagai GTEK berikutnya yang valid. Selanjutnya semua lalu lintas yang dikirim 'nyata' oleh BS tidak dapat lagi didekripsi oleh MS. Dari sudut MSS lalu lintas hanya melihat dari musuh tersebut valid. Untuk memaksa MSS untuk mendirikan kunci musuh, ada beberapa kemungkinan. Jika pelaksanaannya tidak bekerja dengan benar, kunci dari terakhir dari dua kemudian dikirim pesan perintah update GTEK mungkin sebelumnya menimpa salah satu. Oleh karena itu musuh hanya harus mengirimkannya GTEK pesan perintah update setelah BS ditampilkan pesan pembaruan kunci.

Jika implementasi mengikuti standar, yang diterima key kedua pesan. Yang pasti MS tidak akan membentuk 'nyata' kunci BSS, musuh bisa memalsukan beberapa bagian dari pesan perintah update GTEK BSS. Seperti pesan berubah tidak akan diverifikasi sebagai benar dan dibuang oleh MSS. Setelah ini musuh dapat mengirim GTEK sendiri update pesan perintah yang akan diterima. Dalam koneksi unicast ini bahan keying yang berbeda pada mobile station akan terdeteksi sebagai base station tidak dapat mendekripsi data yang dikirim oleh mobile station. Hal ini menyebabkan pesan TEK valid ditakdirkan untuk MS yang kemudian refresh bahan keyingnya. Karena MBS hanya searah, BS tidak dapat mendeteksi bahwa MS telah berbeda GTEKs.

3. Solusi yang Disarankan

3.1 Pesan Terauthentikasi

Tidak otentik manajemen pesan terkirim pada koneksi manajemen utama atau dasar dapat dengan mudah disahkan menggunakan HMAC atau CMAC digit. Itu harus memutuskan jika otentikasi, juga perlu hingga 168 bit, dapat diterima. Kebanyakan pesan yang sangat pendek sehingga sebuah digit ditambahkan akan meningkatkan pesan ke kelipatan dari ukuran aslinya. Karena ini fakta tradeoff harus ditemukan antara keamanan dan efektivitas protokol.



Gambar 2. Solusi Kemungkinan untuk mengirimkan GTEK dalam cara yang aman

Sumber : An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions.

Salah satu cara untuk semacam tradeoff adalah untuk mengotentikasi semua pesan yang dapat memiliki dampak yang serius jika mereka dipalsukan. Selain pesan manajemen yang telah dilindungi oleh otentikasi sebuah angka, ini termasuk semua pesan yang disajikan dalam bagian 2.1. Pesan manajemen lain dapat tetap terauthentikasi. Untuk tahan ukuran pesan secara keseluruhan, CMAC atau tuple HMAC pendek harus digunakan karena memiliki ukuran yang jauh lebih rendah sebagai HMAC penuh.

HMAC didasarkan pada algoritma-1 SHA sehingga ukuran MAC 128 bit dicapai. Untuk HMAC Pendek nilai ini dipotong menjadi 64 bit. Dengan semua parameter yang diperlukan lainnya (paket yaitu jumlah, nomor urutan kunci dan bidang reserved) ini menghasilkan HMAC Pendek digest dari 104 bit. CMAC menggunakan AES128 yang juga menghasilkan nilai bit 128. Untuk CMAC akhirnya digunakan nilai ini dipotong menjadi 64 bit. Dengan semua informasi tambahan yang CMAC lengkap digest juga secara total 104 bit.

Pesan yang ditampilkan memiliki masalah otentikasi, mereka tidak sepenuhnya aman ketika kunci simetris yang digunakan karena kunci ini harus dimiliki oleh semua anggota kelompok. Ini memberikan kemungkinan bahwa pesan dapat dipalsukan oleh setiap anggota grup. Namun, solusi simetris sangat cepat dapat diolah dan melindungi terhadap pemalsuan pesan dari luar grup. Ini adalah kemungkinan untuk meningkatkan keamanan secara signifikan tanpa perlindungan yang lengkap tetapi persyaratan rendah.

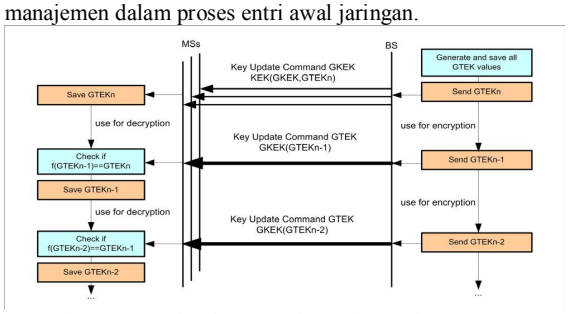
Kemungkinan lain penggunaan akan kriptografi asimetris. Dalam hal ini pesan ditampilkan disahkan oleh tanda tangan yang dibuat dengan kunci pribadi base station. Untuk stasiun mobile ini membutuhkan tanda tangan asimetris untuk memverifikasi dengan kunci publik diketahui ketika mereka menerima pesan seperti ditampilkan manajemen. Namun, solusi ini memiliki kelemahan besar yang membutuhkan waktu banyak yang harus dilakukan dan kunci asimetris harus dikelola. Selain itu otentikasi terjadi sangat sering dan dengan demikian meningkatkan kebutuhan.

3.2 Mananajemen Komunikasi tak Terenkripsi

Untuk melindungi lalu lintas manajemen dari yang dibaca oleh musuh, semua komunikasi manajemen harus dienkripsi. Enkripsi ini dapat menerapkan langsung setelah kedua belah pihak telah membentuk kunci yang sama (yaitu AK otorisasi kunci). Seperti kunci yang sama dibuat, setelah proses otentikasi maka pertukaran TEK berikut dan proses pendaftaran serta semua manajemen selanjutnya komunikasi bisa dienkripsi. Untuk menghindari AK menjadi terlalu sering diperbarui, baik asosiasi keamanan untuk setiap koneksi manajemen dapat ditentukan (CID primer dan dasar yaitu), atau asosiasi keamanan manajemen global baik untuk koneksi manajemen juga akan memadai.

Mengenkripsi payload manajemen pesan tidak memperkenalkan overhead sambungan. Ini hanya memerlukan enkripsi dan dekripsi pesan. Karena mungkin untuk menggunakan kunci simetris, dekripsi dapat diproses sangat cepat.

Solusi seperti menyembunyikan rahasia informasi manajemen, melindungi terhadap mendengarkan yang tidak diinginkan dan tidak mengungkapkan data manajemen untuk membuat profil. Dalam [4], salah satu solusi yang mungkin disajikan untuk mengenkripsi awal informasi manajemen dalam proses entri awal jaringan.



Gambar 3. Menghindari pemalsuan kunci dengan rantai hash GTEK

Sumber : An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions

3.3 Shared Kunci pada Layanan Multi dan Broadcast

Enkripsi Secure data sulit ditransfer melalui MBS. Kunci bersama tidak dapat digunakan karena setiap anggota kelompok bisa membina pesan bila ada arus kunci simetris.

Tapi apa yang dapat dihindari adalah distribusi pesan palsu perintah update kunci yang memungkinkan musuh untuk mengambil kendali atas konten data pada koneksi MBS. Salah satu kemungkinan untuk mencapai ini adalah menghindari update kunci untuk ditampilkan. Sebaliknya update GTEK pesan perintah dapat dikirim ke setiap MS dengan cara unicast seperti pesan perintah update GKEK. Kuncinya kemudian

harus dienkripsi dengan KEK MS-istimewa yang hanya diketahui oleh MS ini individu.

Dibandingkan dengan Request / Reply algoritma ini masih menyimpan setengah dari bandwidth karena tidak ada pesan permintaan yang diperlukan. BS mengirimkan pesan GTEK perintah update dengan sendirinya ketika masa kunci berjalan akan berakhir. Sisi kiri dari Gambar 2 menunjukkan solusi ini dibandingkan dengan pesan update GKEK perintah yang bekerja dengan cara yang sama.

Solusi lain adalah penggunaan kriptografi kunci publik. Di sini perintah pesan update GTEK tetap ditayangkan dan terenkripsi bersama dengan kunci GKEK tetapi tambahan ditandatangani oleh tanda tangan asimetris. MSS menerima pesan GTEK update perintah dapat memverifikasi tanda tangan dari BS dan kemudian mendekripsi GTEK dengan GKEK bersama. Sisi kanan Gambar 2 menunjukkan metode ini bersama-sama dengan pesan perintah update GKEK unicasted.

Kemungkinan ketiga adalah untuk menghasilkan GTEKs sebagai bagian dari rantai hash. Di sini pertama BS membuat nomor acak yang mewakili GTEK0 kunci awal. Kemudian GTEKs lainnya dihasilkan dengan menerapkan fungsi salah satu cara hash ke masing-masing GTEKs sebelumnya. Ini adalah n kali iterasi.

Rantai hash ini memungkinkan untuk memverifikasi setiap GTEK dengan menerapkan fungsi salah satu cara yang sama ke yang sebelumnya. Untuk mencapai hal ini otentikasi dirantai yang GTEK terakhir harus didistribusikan ke masing-masing MS dalam cara yang aman karena merupakan satu-satunya kunci dalam rantai yang tidak dapat disahkan oleh satu sama lain. Satu kemungkinan adalah mendistribusikan untuk GTEKn dalam pesan perintah update GKEK yang merupakan pesan unicast dan terenkripsi dengan kunci MS terkait.

Tabel 1. Perbandingan solusi yang diusulkan erentanan kunci

Sumber: Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol.

Jika MS menerima GTEK baru melalui pesan perintah update GTEK ditayangkan dapat memverifikasi integritas dengan menerapkan salah satu cara fungsi hash f untuk itu. Jika otentikasi yang positif, GTEK saat ini dapat ditimpa dan yang diterima dibuat. Jika otentikasi gagal, MS membuang pesan dan permintaan sebuah GTEK baru melalui permintaan unicast / mekanisme Balas. Gambar 3 menunjukkan perilaku ini.

Untuk menerapkan algoritma ini, update GKEK pesan perintah kunci harus mampu mengangkut GKEK dan kunci GTEK bersama-sama. Desain pesan perintah update kunci sudah termasuk kunci sehingga hanya sedikit modifikasi yang diperlukan di sini. Selain itu keadaan GTEK mesin di BS harus menghasilkan rantai hash GTEK dan menyimpan semua kunci. Keadaan mesin GTEK di MS harus menambahkan fungsi untuk otentikasi kunci GTEK dengan menghitung fungsi hash dan membandingkannya dengan kunci sebelumnya.

Salah satu kelemahan algoritma ini adalah bahwa ia memiliki meneruskan menurunkan kerahasiaan. Ini berarti MS, bergabung ke grup, dapat mendekripsi semua data ditayangkan sejak generasi rantai terakhir hash. Jika meneruskan kerahasiaan sangat penting, rantai hash harus diregenerasi setiap kali memasuki MS grup.

Pada Tabel 1 untuk membandingkan solusi yang karakteristiknya berbeda yang kontras satu sama lain. Pertama diperkenalkan lalu lintas setiap solusi yang akan didiskusikan. Untuk distribusikan kunci dalam perilaku unicast kebutuhan satu update kunci per mobile station. Ini berarti lalu lintas diperkenalkan langsung sesuai dengan ukuran kelompok n. Bila menggunakan tanda tangan asimetris atau rantai hash untuk otentikasi transfer GTEK, hanya satu pesan diperlukan untuk memperbarui kunci dari semua stasiun bergerak karena penyiaran.

Dengan demikian lalu lintas pada solusi ini diperkenalkan adalah konstan dan tidak tergantung pada jumlah anggota dalam kelompok. Fakta lain yang penting adalah kebutuhan komputasi dari algoritma yang berbeda untuk stasiun bergerak dan stasiun base. Terutama stasiun bergerak tidak boleh sibuk dengan perhitungan rumit untuk menghemat daya baterai.

Untuk eksklusif unicasting stasiun mobile hanya perlu memverifikasi HMAC dan menyimpan kunci. Oleh karena itu, daya komputasi yang dibutuhkan sangat rendah. Juga penggunaan rantai hash tidak memerlukan banyak perhitungan. Di sini stasiun mobile menghitung untuk fungsi hash dari kunci diterima dan membandingkannya dengan kunci disimpan.

Untuk kedua solusi persyaratan untuk stasiun basis juga sangat rendah. Untuk unicasting eksklusif, kunci baru dihasilkan secara acak, untuk rantai hashnya kemudian dihitung dengan fungsi hash. Ketika tanda tangan asimetris digunakan, kebutuhan

komputasi jauh lebih tinggi. Dalam pengukuran laboratorium sendiri ditetapkan bahwa waktu untuk memverifikasi tanda tangan asimetris adalah sekitar 20 kali lebih tinggi dibandingkan verifikasi dengan HMAC digit. Juga persyaratan untuk stasiun pangkalan untuk membuat tanda tangan asimetris dengan itu kunci pribadi adalah sekitar 900 kali lebih tinggi dibandingkan dengan penciptaan HMAC digit. Namun, base station dapat diasumsikan memiliki daya komputasi yang lebih banyak dan tanda tangan asimetris harus dibuat hanya sekali per update GTEK dari semua stasiun mobile.

Akhirnya kerahasiaan dari solusi harus dianalisis. Semua solusi dan juga MBRA saat ini didefinisikan tidak dapat menyediakan kerahasiaan. Setiap algoritma memiliki periode di mana sebelumnya data yang dikirim dapat didekripsi oleh stasiun mobile yang bergabung dengan grup. Untuk unicasting eksklusif dan solusi asimetris periode ini adalah masa salah satu GTEK. Ini berarti bahwa sebuah stasiun mobile yang bergabung kelompok dapat mendekripsi semua lalu lintas yang dienkripsi dengan GTEK saat ini digunakan. Ketika otentikasi didasarkan pada rantai hash, periode ini berlangsung untuk masa satu rantai hash lengkap. Karena key rangkaian langsung dengan fungsi hash satu cara yang dikenal, sebuah stasiun mobile yang bergabung dengan kelompok dapat dengan mudah menghitung semua GTEKs sebelumnya dalam rantai hash saat ini.

4. Kesimpulan

Dalam tulisan ini, menunjukkan kerentanan keamanan yang berbeda ditemukan di 802.16e IEEE dan memberikan solusi yang mungkin untuk menghilangkannya. Ketika semua perubahan yang diajukan diterapkan, keamanan Mobile WiMAX dapat meningkat secara signifikan.

Enkripsi komunikasi manajemen memecahkan kerentanan yang ada sejak versi standar pertama. Dengan enkripsi yang digunakan musuh tidak lagi dapat mengumpulkan informasi manajemen tentang perangkat mobile.

Beberapa pesan ditemukan yang membawa informasi sensitif tanpa otentikasi apapun. Jika pesan diterima ini bisa berbahaya bagi sistem operasi. Jika otentikasi pesan diperluas untuk pesan-pesan seperti yang diusulkan, pesan tersebut dilindungi terhadap pemalsuan. Untuk mencegah penyalahgunaan kunci dalam siaran-multi dan algoritma rekeying tiga solusi yang berbeda disajikan berdasarkan unicasting, kriptografi asimetris dan hash chaining.

Membangkitkan kunci enkripsi lalu lintas di suatu rantai hash adalah solusi cepat yang tidak memperkenalkan banyak overhead. Sayangnya memiliki waktu yang lama tanpa kerahasiaan. Jadi jika kerahasiaan merupakan salah satu terpenting dari algoritma lain yang mungkin sesuai.

Daftar Pustaka :

[1] IEEE Std. 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks, part 16, Air Interface for Fixed Broadband Wireless Access Systems, IEEE Press, 2004.

[2] IEEE Std. 802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks, part 16, Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Press, 2006.

[3] Johnston D., Walker J.: Overview of IEEE 802.16 Security, IEEE Computer Society, 2004.

[4] Taeshik Shon, Wook Choi: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, First International Conference, NBiS 2007, LNCS, Vol. 4650, pp. 88-97, 2007

[5] Datta A., He C., Mitchell J.C., Roy A., Sundararajan M.: 802.16e Notes, Electrical Engineering and Computer Science Departments, Stanford University, CA, USA, 2005, available at http://www.iab.org/liaisons/ieee/EAP/802.16e Notes.pdf

[6] Yuksel E.: Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling, Technical University Denmark, DTU, 2007, available at http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5159

[7] Ju-Yi Kuo: Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol, Stanford University, CA, USA, 2006, available at http://www.stanford.edu/class/cs259/projects/project01/01-Writeup.pdf

[8] Krawczyk H., Ballare M., Canetti R.: HMAC: Key-Hashing for Message Authentication, RFC 2104, http://www.ietf.org/rfc/rfc2104.txt, IETF, 1997.

[9] Dworkin M.: Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, NIST special publication 800-38B, National Institute of Standards and Technology (NIST), MD, USA, 2005