Análise do Estabelecimento de Associações Seguras em Sistemas Móveis de 3ª Geração

Fabrício J. L. Ribeiro, Jaime C. R. Lopes e Aloysio de C. P. Pedroza[1]

***Resumo*-- Este artigo apresenta uma análise de protocolos utilizados no estabelecimento de associações seguras em sistemas móveis de terceira geração (3G), através de um estudo de modelagem formal utilizando a linguagem LOTOS. Os protocolos visam atender os requisitos de segurança da rede de 3ª Geração. A arquitetura utilizada para a implementação destes protocolos tem suas premissas definidas no fórum de discussão de 3G. Os resultados obtidos demostram que a descrição formal é de grande valia para a validação da segurança provida pelos protocolos.**

***Abstract*-- This paper shows the modeling of 3rd generation mobile systems protocols using a formal description technique based on the LOTOS language. These protocols are devised to achieve the 3rd Generation network security requirements. The architecture used in this implementation is well defined in the 3G-discussion forum. The results show that formal descriptions techniques are very usefull to validate the protocols security guarantee.**

***Index Terms*—Communication system security, Data security, Finite state machines, Protocols, Specification languages.**

I. Introdução

A necessidade de confiabilidade e segurança é preocupação constante em todos os ambientes. Com o desenvolvimento da telefonia móvel celular, que propiciou a universalização nas comunicações de voz, a comunicação móvel de dados recebeu impulso no sentido de atingir a ubiqüidade. Para este fim, e considerando a demanda crescente dos usuários por aplicações com elevada qualidade de apresentação gráfica e sonora, incluindo diversos recursos multimídia, está em desenvolvimento e formulação a arquitetura universal de sistemas de telecomunicações (UMTS – Universal Mobile Telecommunication Systems).

Se a segunda geração (2G) trouxe a telefonia móvel para o mercado em geral, espera-se que a arquitetura de terceira geração (3G) estenda-se além da telefonia e abranja o fornecimento de comunicação de dados em alta velocidade. Essa arquitetura de terceira geração vem sendo desenvolvida pelo grupo de trabalho 3GPP (Third Generation Partnership Project).

A arquitetura de 3G pretende tornar a comunicação universal e transparente ao usuário, independente de plataforma de hardware, sistema operacional ou tipo de equipamento, móvel ou fixo. Seu desenvolvimento, entretanto, envolverá alterações significativas na base de equipamentos sem fio instalada. O núcleo dessa rede deverá mudar de comutação de circuitos para comutação de pacotes, além de que deverá ser construído de forma a operar independente da tecnologia de acesso empregada.

A arquitetura de terceira geração deverá ser baseada em uma rede IP, já que este protocolo tornou-se o protocolo universal para comunicações em rede. O uso de pacotes IP na estrutura de transmissão de dados e de sinalização apresenta-se como caminho natural para a convergência entre as redes fixas e móveis. Esta convergência acontecerá pela padronização de uma arquitetura totalmente baseada no protocolo IP, que incluirá o sistema celular, as redes fixas e as redes locais sem fio. Sendo assim, muitos dos requisitos de segurança atualmente existentes, ou em definição, deverão também seguir os aspectos já adotados nas redes convencionais e balizar o desenvolvimento dos seus análogos para redes móveis.

O desenvolvimento de um modelo padrão para protocolos de segurança de terceira geração deverá se basear, necessariamente, na arquitetura de segurança IP (IPSec) [1] para garantir às redes sem fio a interoperabilidade com os serviços já utilizados nas redes atuais. A arquitetura necessária ao desenvolvimento de tais garantias deve ser organizada em camadas, cada uma delas provendo parte da segurança requerida. Tais camadas apresentarão um protocolo de sinalização e funções diversas de monitoramento no domínio da operadora, e cada uma delas terá seus requisitos definidos com base em padrões de segurança desejados. Por outro lado, pelas limitações de vulnerabilidade e banda dos sistemas sem fio, a sinalização deve apresentar alta complexidade e gerar pequeno volume de tráfego adicional.

Com o desenvolvimento da 3ª geração de sistemas móveis, vem crescendo a demanda por segurança. Assim, foram definidos pontos cruciais para garantia de segurança do sistema como um todo, conforme visto na figura 1:

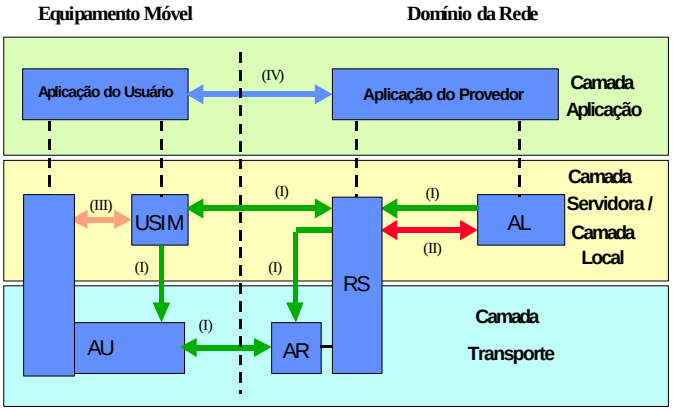
- Segurança no Acesso a Rede (I);
- Segurança na Rede (II);
- Segurança ao Usuário (III);
- Segurança nas Aplicações (IV).

[1] F. J. L. Ribeiro é aluno do Curso de Mestrado do Grupo de Teleinformática e Automação (GTA) do Programa de Engenharia Elétrica – COPPE-Poli/UFRJ (e-mail: fabricio@gta.ufrj.br)

J. C. R. Lopes é aluno do Curso de Mestrado do Grupo de Teleinformática e Automação (GTA) do Programa de Engenharia Elétrica – COPPE-Poli/UFRJ (e-mail: jaime@gta.ufrj.br)

A. de C. P. Pedroza, Ph.D. é professor do Programa de Engenharia Elétrica – COPPE-Poli/UFRJ (e-mail: aloysio@gta.ufrj.br)

Universidade Federal do Rio de Janeiro
Caixa Postal. 68504 – CEP 21945-970
Rio de Janeiro – RJ - Brasil



Legenda:
AU – Agente de Usuário
AR - Autenticação de Rede
AL - Ambiente Local
RS - Rede Servidora
USIM - Módulo de Identificação de Usuário UMTS

Fig. 1. Visão geral da arquitetura de segurança 3G.

Como a comunicação móvel, pelas suas restrições inerentes anteriormente relacionadas, apresenta cada vez mais uma complexidade sistêmica, o nível de abstração necessário à produção de definições e padrões eleva-se. O foco muda, passando para a definição abstrata de funcionalidades de um serviço. A verificação das propriedades de segurança de um protocolo, beneficiar-se-á de uma especificação mais formal.

Nesse sentido, a especificação e a verificação de protocolos envolvidos nos processos de garantia de segurança deve ser orientada por técnicas de descrição formal, empregando mecanismos e linguagens apropriados. As técnicas de descrição formal, por serem métodos de definição do comportamento de um sistema com o uso de uma sintaxe e de uma semântica, permitem uma implementação de protocolos sem ambigüidades, precisa e completa. Além disso, provêem uma base bem definida para a verificação e validação desses protocolos, entendidas como a avaliação de conformidade dos mesmos com relação ao comportamento esperado [2]-[3].

Nossa abordagem consiste na modelagem de protocolos de segurança com o uso de uma técnica de descrição formal, baseado na linguagem LOTOS, e na análise destes protocolos usando as ferramentas contidas no pacote denominado CADP [2].

O restante deste artigo está organizado nas seguintes seções: a seção 2, mostra como é a aplicação da técnica de descrição formal em protocolos apresentando uma visão geral da linguagem LOTOS e da ferramenta de análise CADP. Na seção 3, apresentamos os fundamentos da arquitetura de segurança de terceira geração. Na seção 4, mostramos como é a análise dos protocolos. A seção 5 apresenta os resultados obtidos, enquanto a seção 6 contém a conclusão e temas para trabalhos futuros.

II. Aplicação de TDF nas Comunicações Seguras

As técnicas de descrição formal tornam possível a captura do comportamento funcional de sistemas [4], e, em particular, de protocolos de segurança.

A apropriada captura das propriedades desejadas do sistema, bem como a sua especificação formal adequada, são essenciais à produção de documentação sem ambigüidades.

A. A Linguagem LOTOS e a Ferramenta CADP

LOTOS (Language Of Temporal Ordering Specification) é uma Técnica de Descrição Formal padronizada pela ISO (International Standards Organization), utilizada na descrição formal de sistemas abertos [3]. Seu projeto foi motivado pela necessidade de uma linguagem que oferecesse alto nível de abstração sobre uma forte base matemática. Os modelos em LOTOS permitem o uso de várias técnicas de validação e verificação, e diversas ferramentas foram desenvolvidas para a automatização destes processos.

A parte de dados da linguagem é baseada na teoria de tipos de dados algébricos abstratos, mais especificamente na linguagem de especificação ACTONE [5]. Os tipos de dados abstratos descrevem os valores que os dados podem assumir e as operações que sobre eles atuam, sem especificar como são representados e manipulados na memória, o que contribui para a abstração inerente à linguagem [2]. Já a parte comportamental do LOTOS é baseada na álgebra de processos, combinando características das linguagens CCS [6], de Milner, e CSP, de Hoare. Um sistema concorrente é descrito como uma coleção de processos paralelos interagindo por meio de *rendezvous* (pontos de encontro). O comportamento de cada processo é especificado com o uso de uma álgebra de operadores (vide Tabela 1), e os processos podem manipular e trocar dados em pontos de interação denominados portas (*gates*) [3].

TABELA I
Operadores LOTOS.

OPERADORES	INTERPRETAÇÃO
P !V ?Y:T; A	Interação pela porta P, enviando um valor V e recebendo uma variável Y de valor T, com execução da ação A
A [ ] B	Executa A ou B
A |[h,i,j]| B	Executa A e B em paralelo, com sincronização nas portas h,i,j
A ||| B	Executa a ou B em paralelo, sem sincronização
exit	Termina com sucesso
P [h,i,j] (H,I,J)	Chamada do processo com parâmetros das portas h,i,j e parâmetros de valores H,I,J

Para analisar o comportamento de um protocolo, empregando uma especificação LOTOS, utilizamos a ferramenta CADP (Caesar/Aldebaran Development Package) [2]. O CADP oferece um conjunto integrado de funcionalidades, que vão da simulação interativa até a verificação baseada em modelos. Este processo pode ser visualizado na figura 2.

As funcionalidades apresentadas pelo CADP podem ser reunidas sob três grandes grupos:

- Compilação de especificações descritas em LOTOS;
- Verificação de sistemas comunicantes;
- Validação e teste de protocolos.

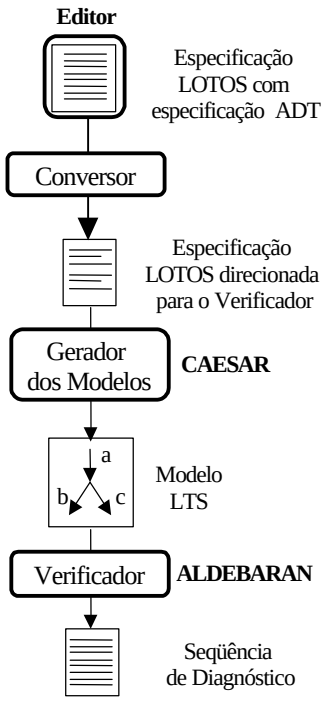


Fig. 2. Processo de análise empregando as ferramentas do pacote CADP.

Na verificação de sistemas comunicantes, a partir da obtenção de sistemas de transições rotuladas, pode-se promover a verificação de várias relações de equivalência (equivalência forte, equivalência observacional, equivalência de segurança, dentre outras). A validação e testes de protocolos permitem a inserção de operadores lógicos temporais. Tais operadores são aplicados sobre sistemas de transições rotuladas, possibilitando a verificação de propriedades nos protocolos especificados.

B. Aspectos de Segurança

Uma análise do comportamento dos protocolos que promovem as garantias de segurança deve estar de acordo com os requisitos determinados pelo sistema. O processo de análise formal para protocolos adequa-se a este esforço de se atestar a segurança de sistema de comunicação sem fio. A especificação de um protocolo com o conceito de entidades confiáveis e não confiáveis torna-se viável devido à flexibilidade, em LOTOS, dos tipos de dados abstratos [7].

O processo de validação e a formalização das propriedades de segurança definem uma ordem de estados que acarreta em uma comunicação segura, sendo esta ordem avaliada através das propriedades que são capazes de expressar eventos de segurança. No entanto, este processo pode acarretar modelos infinitos, sendo assim, necessário efetuar alguma simplificação. Esta simplificação é viável pela limitação do número das entidades envolvidas.

A estrutura da especificação é composta por vários processos que interagem entre si através das portas de comunicação existentes no protocolo. Cada entidade envolvida é modelada pelo processo que descreve o seu exato comportamento.

A especificação formal permite, de um modo abstrato, a obtenção de todos os detalhes dos mecanismos de segurança. Assim, podemos focar somente nos serviços realmente seguros. A verificação de que todos os eventos no protocolo são seguros, atesta a segurança deste protocolo.

III. Comunicações Seguras nos Sistemas Móveis de 3ª Geração

Para ilustrar como poderão ser analisadas as garantias de segurança, assumimos que, com as definições de características de segurança da rede 3G [8]-[9], podemos modelar um interceptador (invasor) na tentativa de invasão [10]. Ele não poderá se autenticar, quebrar a chave criptográfica de segurança do sistema nem conseguir trocar sinalização sem ter a informação da chave criptográfica.

Muitas propriedades seguras podem ser verificadas [7]. Estas propriedades são estados que podem acontecer sem prejuízo da segurança no sistema. A autenticação, o controle de acesso e a integridade são propriedades de segurança. Cada um desses serviços de segurança necessita de um estado particular que pode acontecer ou não.

Vamos considerar um protocolo de autenticação atuando entre duas entidades, sendo uma delas um provedor de domínio de rede que deve autenticar um usuário. Há dois pontos críticos nesta situação: o primeiro ocorre quando se inicia a autenticação e o segundo, quando é assegurada a identificação do usuário [11].

A. Modelo UMTS para Domínios Seguros

Uma fraqueza identificada no sistema de 2ª geração é a falta de segurança no núcleo da rede. Isto não foi tratado como um grande problema, pois os sistemas de 2ª geração eram compostos por sistemas proprietários e controlados por um número reduzido de instituições. Agora, com a introdução do backbone IP [9], não somente usado para o tráfego de sinalização mas também para o tráfego de usuários, novas ameaças e riscos surgem para o sistema.

Os serviços seguros têm necessidade de confiabilidade, integridade e autenticação. Isto será assegurado com procedimentos padronizados e baseados em técnicas de criptografia. Estes procedimentos acarretam a implementação dos domínios seguros [1].

Estes domínios são gerenciados por uma única autoridade

que define a política de segurança a ser implementada. O controle dos níveis de segurança é determinado por esta política e implementado pelos dispositivos de borda (*Security Gateways* - SEGs). Os SEGs são responsáveis pela integridade e a autenticação dos dados de origem.

O domínio de rede UMTS deve ser dividido logicamente e fisicamente em domínios seguros. Este controle dos domínios seguros deve corresponder ao núcleo da rede e a sua separação deve ser realizada pelos roteadores de borda (SEGs).

1) Roteadores de Borda Seguros

Os SEGs são entidades na borda dos domínios seguros que serão usadas pelos protocolos baseados em IP [9]. Controlam as comunicações entre domínios diferentes (interface Za) e entre SEGs e entidades de rede internas no domínio (interface Zb), conforme a figura 3.

Todo tráfego IP dos domínios seguros deve passar por estes roteadores de borda, sendo a determinação do número destes dispositivos dependente da necessidade do equilíbrio entre a acessibilidade externa e o balanceamento de carga, para evitar um único ponto de falha. Os SEGs são responsáveis por executar a política de segurança nas comunicações entre as redes.

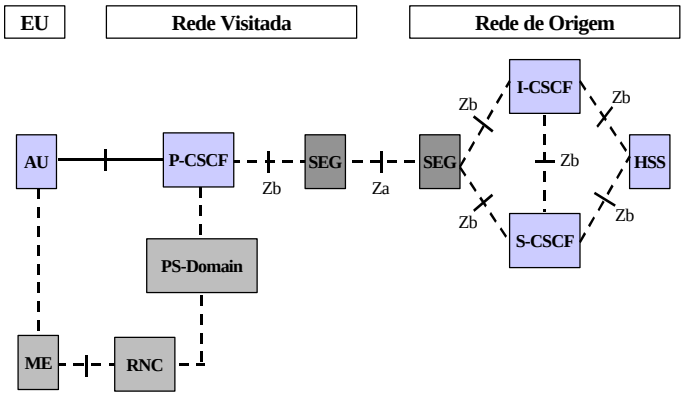


Fig. 3: Arquitetura 3G dos domínios seguros

No modelo de segurança proposto para os sistemas de 3ª geração, estes dispositivos de borda devem ter capacidade de oferecer armazenamento seguro das chaves de autenticação usadas no protocolo IKE [12].

B. Associações Seguras (SAs)

A arquitetura IPSec proporciona segurança aos serviços através do estabelecimento de associações seguras. Estas associações são conexões unidirecionais, protegidas criptograficamente, que são identificadas através das SPI (*Security Parameter Index*).

Na arquitetura UMTS [13], o estabelecimento das SAs poderá ser baseado no protocolo de troca de chaves da Internet (*Internet Key Exchange* – IKE) [12]. Este protocolo tem como objetivo principal negociar, estabelecer e manter associações seguras.

Em uma comunicação segura estabelecida entre dois SEGs, o gerenciamento e a distribuição das chaves poderão ser realizados pelo ISAKMP (Internet *Security Association* and *Key Management Protocol*) [14], que é fundamental para o estabelecimento das duas associações IPSec (uma em cada direção).

A criação de uma associação segura é composta por duas fases: ISAKMP AS e IPSec AS.

1) IKE Fase 1 – ISAKMP AS

Nesta fase, é realizada a autenticação mútua e o estabelecimento das chaves criptográficas, que pode acontecer de dois modos, o agressivo e o principal.

No modo principal, são trocadas seis mensagens, onde são enviados *cookies* e acordado o algoritmo de criptografia, através de troca Diffie-Hellman [15], que resulta em uma chave para criptografar as identidades nas mensagens. No modo agressivo, só há troca de três mensagens.

2) IKE Fase 2 – IPSec AS

Nesta fase, também conhecida como modo rápido de troca, é estabelecida uma associação ESP (IP *Encapsulating Security Payload*) [16] ou AH (IP *Authentication Header*) [17], que envolve negociação de parâmetros de criptografia e escolha dos valores dos SPI em cada direção da comunicação.

IV. Procedimento de Análise

A especificação dos modos de estabelecimento de associações sdeguras em LOTOS permite modelar o comportamento desejado para o serviço, de modo que possa ser comparado com o comportamento obtido para os dois modos do protocolo ISAKMP.

A relação entre diferentes descrições em LOTOS de um dado sistema [18] e, em particular, entre especificações (serviço) e implementações (protocolo) pode ser estudada usando a noção de equivalência, oriunda do CCS [6]. Essa equivalência, conhecida como observacional, é baseada na idéia de que o comportamento de um sistema é determinado pelo modo pelo qual ele interage com os observadores externos. A teoria de equivalência permite não somente provar que uma implementação está correta, com respeito a uma dada especificação, mas também substituir sistemas complexos por outros mais simples e de comportamento equivalente [3].

As outras duas equivalências analisadas, a equivalência forte (ou bissimulação forte) e a com segurança, também são ferramentas importantes de análise. A equivalência forte, entretanto, caracterizada por uma elegante definição de ponto fixo, é muito forte do ponto de vista de verificação de programas. Não leva em consideração critérios de abstração, especialmente o conceito de ações internas ou não observáveis [2]-[6]. A equivalência forte, em outras palavras, exige que toda ação interna de um processo seja igualmente realizada por uma ação interna de outro processo [4]. Como a especificação do serviço é uma modelagem do comportamento externamente observável do protocolo, não contém necessariamente as mesmas transições nem passa pelos mesmos estados internos que o protocolo modelado.

Para ilustrar o método abordado no trabalho, esta seção apresenta um exemplo de análise. Foi escolhida a parte inicial do estabelecimento das associações seguras, realizado pelo protocolo ISAKMP [14]. Como já foi apresentado, na fase 1

deste processo há dois modos de operação (principal e agressivo), utilizados para demonstrar o quanto pode variar o comportamento de um protocolo em suas características de segurança com a simples determinação do modo de funcionamento.

Este artigo apresenta uma visão do processo baseada em estudos já realizados [7]-[19]-[20]. Na análise formal de protocolos que utilizam criptografia como base da garantia da segurança, verificamos que o ponto fraco se encontra justamente durante o processo de estabelecimento e negociação das características de segurança que serão adotadas. É neste ponto em que geralmente se encontra a vulnerabilidade nos processos seguros.

O número e a complexidade das mensagens compostas por cada estabelecimento das associações influenciam diretamente a ação de intrusos na interceptação, modificação e retransmissão de mensagens . O grande problema encontrado é que, quanto maior a robustez de um sistema, mais complexa é sua implementação. Achar este equilíbrio é cada vez mais uma necessidade [20].

A. Estudo de Caso do Protocolo ISAKMP

O protocolo ISAKMP é definido para prestar um serviço necessário ao atendimento a requisitos de troca de chaves criptográficas. Durante este processo, os SEGs trocam informações para estabelecimento de associações seguras através das interfaces Za (vide figura 4).

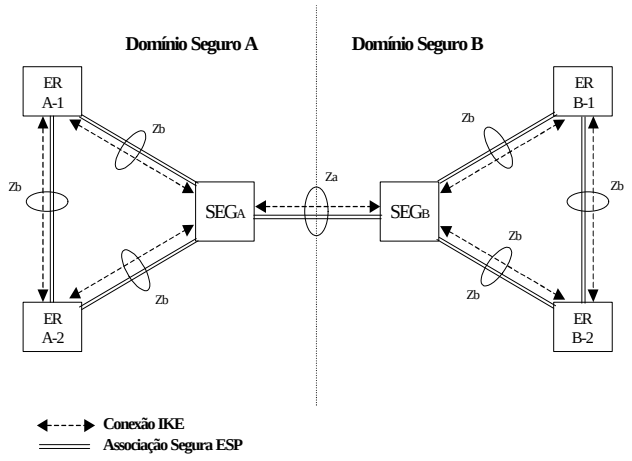


Fig. 4: Entidades envolvidas no processo de associação entre domínios seguros

Assim, conforme apresentado na figura 5, para iniciar uma negociação no modo agressivo, o SEG_A envia na mensagem 1 o seu *cookie* C_{SEGA} e a identificação ID_{SEGA}. Inicia-se, então, a troca Diffie-Hellman [15] para estabelecer a chave criptográfica. O SEG_B aceita o tipo de criptografia, valida a identificação recebida e envia, na mensagem 2, os *cookies* C_{SEGB} e C_{SEGA} e as identificações ID_{SEGA} e ID_{SEGB}. Então o SEG_A valida a identificação e envia na mensagem 3 a confirmação criptografada com a chave acordada.

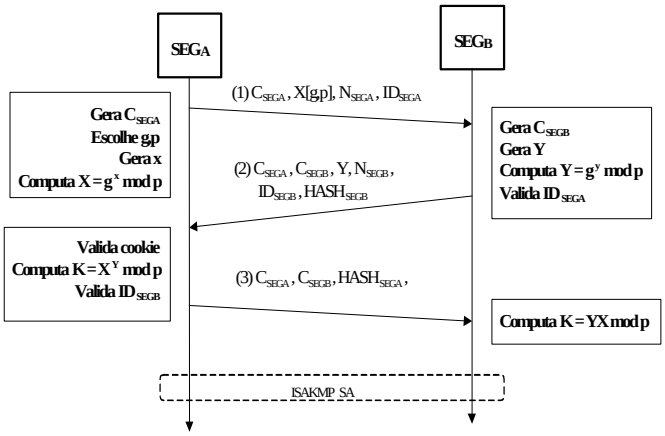


Fig. 5: Modo agressivo de estabelecimento de associações seguras

Já no modo principal apresentado na figura 6, a negociação é iniciada pelo envio, no primeiro par de mensagens, dos *cookies* (C_{SEGA} e C_{SEGB}) e do tipo de criptografia suportado. Nas mensagens 3 e 4, é feita a troca Diffie-Hellman, que resulta em uma chave utilizada para criptografar as identidades (ID_{SEGA} e ID_{SEGB}). A confirmação é feita com o envio criptografado das identidades nas mensagens 5 e 6.

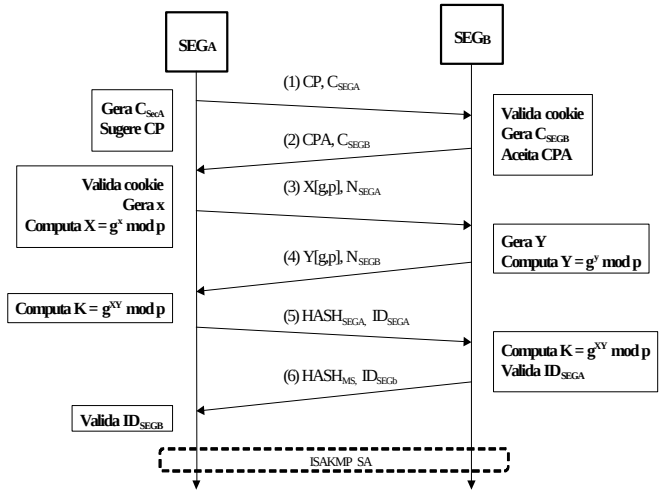


Fig. 6: Modo principal de estabelecimento de associações seguras

1) A Especificação LOTOS para o Estabelecimento de Associações Seguras em Modo Agressivo e Principal

Na especificação elaborada, foram definidos processos que implementam o protocolo ISAKMP, interligados por meio de comunicações simples e executados por dois roteadores de borda seguros (SEGs). Estes roteadores trocam as mensagens apresentadas nas figuras 5 e 6.

A arquitetura empregada para o estabelecimento de comunicações em modo seguro é descrita em LOTOS pela expressão comportamental do serviço, que é idêntica nos dois modos de operação.

A modelagem em LOTOS do serviço que representa o comportamento esperado nos dois modos de operação pode ser visto abaixo:

```
specification isa_serv [ACC, DEL] : noexit

library
isa_lib
endlib

behaviour
  Service [ACC, DEL]
where

  process Service [ACC, DEL] : noexit :=
    ACC ?datos:data_type;
      DEL !datos;
        Service [ACC, DEL]
  endproc
endspec
```

A seguir, apresentamos um fragmento da especificação LOTOS, contendo o comportamento do protocolo:

```
behaviour
hide tp_datareq1, tp_dataind1, tp_datareq2, tp_dataind2, isa_req,
isa_cnf, isa_ind, isa_res   in
    (
     (
      SEG_A [ACC, isa_req, isa_cnf]
      |||
      SEG_B [isa_ind, DEL, isa_res]
     )
     |[isa_req, isa_cnf, isa_ind, isa_res]|
     (
      ISA_A [isa_req, isa_cnf, tp_datareq1, tp_dataind1]
      |||
      ISA_B [isa_ind, isa_res, tp_datareq2, tp_dataind2]
     )
     |[tp_datareq1, tp_dataind1, tp_datareq2, tp_dataind2]|
      TP [tp_datareq1, tp_dataind1, tp_datareq2, tp_dataind2]
```

V. Resultados obtidos

Os resultados obtidos com a verificação do comportamento do protocolo, em relação ao modelo do serviço, podem ser vistos na figura 7 com a análise do número de estados, transições e rótulos do protocolo.

Por se tratar de modos diferentes de execução de um mesmo protocolo, a grande diferença encontrada é a expansão do comportamento dos estados e rótulos que determinam o grau de vulnerabilidade dos modos em relação a interceptações das mensagens. Podemos perceber que o modo principal apresenta um número maior de estados, transições e rótulos, o que lhe confere menor vulnerabilidade a ataques externos.

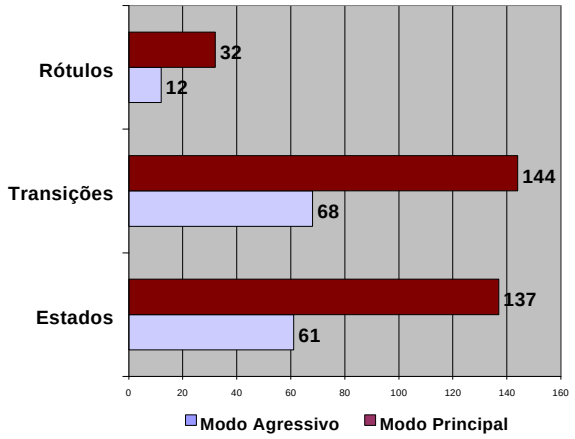


Fig. 7: Número de rótulos, transições e estados nos modos de estabelecimento de associações seguras principal e agressivo

A observação das equivalências, executada com a ferramenta Aldebaran, resultou em que as equivalências observacional e com segurança foram verificadas inteiramente. A equivalência forte, pelo motivo exposto no item IV, não foi verificada integralmente. De fato, existem diferenças entre a evolução do diagrama de estados do protocolo e o do serviço modelado. Diversos estados internos surgem no modelo mais completo (protocolo), que tornam a evolução diferente.

Observamos que, pela modelagem formal de um protocolo, podemos aferir as suas propriedades de segurança, e, através dos estados do protocolo, verificar eventuais falhas nos procedimentos executados por ele.

VI. Conclusão e Trabalhos Futuros

Este artigo apresentou um processo de verificação formal para protocolos de confiabilidade e segurança, utilizando a linguagem LOTOS. A ferramenta CADP possibilitou a correta validação da especificação do protocolo com passagem de dados sem a necessidade da implementação do código. Apresentamos como especificar a fase de estabelecimento de associações seguras, metodologia que pode ser empregada na estrutura de uma camada de serviços de confiabilidade e segurança, pertencente a arquitetura de sistemas móveis de terceira geração (3G).

Foi proposto um processo de validação das propriedades de segurança de um protocolo. Esta validação tem como base a verificação da quantidade dos seus estados e a confirmação das propriedades observacionais. Como foi mostrado, as equivalência observacional e com segurança foram atendidas. A equivalência forte não foi observada devido à simplificação ocorrida durante o processo de minimização, que resultou num diagrama com número de estados muito menor que o original, além de ter sua numeração alterada. As equivalências foram definidas para garantir que o protocolo modelado apresenta, em termos observacionais, o mesmo comportamento que se espera do serviço de segurança modelado.

A análise da quantidade de estados encontrados nos dois modos nos permite afirmar que, devido ao maior número de estados encontrados na utilização do modo principal, este

torna-se menos vulnerável em relação a ataques nesta fase do processo, devido à maior complexidade das mensagens e a variações de estados, que dificultam a correta interceptação por um intruso. Este intruso precisaria dispor de maior poder de processamento para ter sucesso num processo de interceptação no modo principal.

O resultado obtido demonstra que a descrição formal é de grande contribuição para a validação de confiabilidade e segurança dos protocolos no sistema móvel de terceira geração. Pode-se afirmar que trabalhos neste sentido serão fundamentais para o estabelecimento desta nova filosofia de comunicação. Ao nosso ver, estaremos contribuindo com uma metodologia de trabalho e com a validação de protocolos de confiabilidade e segurança que ainda não foram testados no sistema móvel de terceira geração e assim verificando as garantias do atendimento aos requisitos de segurança que sejam necessários.

VII. Referências

[1] S. Kent e R. Atkinson. “Security Architecture for the Internet Protocol”, IETF RFC 2401, Nov. 1998.

[2] J. C. Fernandez, H. Garavel, A. Kerbrat, R. Mateescu, L. Mounier e M. Sighireanu, in: R. Alur e T. Henzinger (Eds.). “CAESAR/ALDEBARAN Development Package: a protocol validation and verification toolbox”. Proceedings of the Eighth Conference on Computer-Aided Verification, LNCS, Springer Verlag, Berlin, 1996.

[3] T. Bolognesi e E. Brinksma. “Introduction to the ISO specification language LOTOS”. Computer Networks and ISDN Systems, 14: 25–59, 1987.

[4] R. Bagatelli, D. F. C. Moura e A. C. P. Pedroza “Especificação Formal de uma Arquitetura de Suporte à Descoberta de Serviços em Redes Móveis Ad Hoc”, in anais do V Workshop de Métodos Formais (WMF'2002), Gramado, RS, Brasil, Out. 2002.

[5] J. de Meer, R. Roth, e S. Vong. “Introduction to Algebraic Specifications Based on the Language ACT ONE”. Computer Networks and ISDN Systems, 23(5): 363-392, 1992.

[6] R. Milner. “Communication and Concurrency”. Prentice-Hall, 1989.

[7] F. Germeau e G. Leduc. “Model-based Design and Verification of Security Protocols using LOTOS”, 1997.

[8] 3G TS 33.102, 2003-03. “3rd Generation Partnership Project; Technical Specification Group; 3G Security Architecture”.

[9] J. Rautpalo, “GPRS Security - Security Remote Connections over GPRS”, 2000.

[10] C. Pecheur, G. Leduc, O. Bonaventure, L. Léonard e E. Koerner. “Model-based verification of a security protocol for conditional access to services”, 1999.

[11] G. Leduc. “Verification of two versions of the Challenge Handshake Authentication Protocol”, 2001.

[12] D. Harkins e D. Carrel, “The Internet Key Exchange (IKE)”, IETF RFC 2409, Nov. 1998.

[13] 3GPP TS 33.210: 2003-06 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security”.

[14] Maughan, D., Schertler, M., Schneider, M. e Turner, J., “Internet Security Association and Key Management Protocol (ISAKMP)”, RFC 2408, Nov. 1998.

[15] W. Diffie e M. E. Hellman, “New Directions in Cryptography,” IEEE Trans. Info. Theory, Vol. 22, Nov. 1976.

[16] S. Kent e R. Atkinson, “IP Encapsulating Security Payload (ESP)”, IETF RFC 2406, Nov. 1998.

[17] S. Kent and R. Atkinson, “IP Authentication Header”, IETF RFC 2402, Nov. 1998.

[18] W. Marrero, E. Clarke, e S. Jha. “A Model Checker for Authentication Protocols”. Proc. of the DIMACS Workshop on Design and Formal Verification of Security Protocols, Rutgers University, Set. 1997.

[19] G. Leduc, O. Bonaventure, L. Léonard, E. Koerner e C. Pecheur. “Model-based Design and Verification of security protocols for conditional access to services”, 1999.

[20] F. J. L Ribeiro, J. C. R. Lopes, e A. C. Pedroza, – “Análise dos Processos de Segurança em Sistemas Móveis de 3ª Geração”, in anais da I Escola Regional de Redes de Computadores - ERRC 2003, Porto Alegre, RS, Brasil, Set. 2003.