Um Mecanismo de Proteção de Nonces para a Melhoria da Segurança de Redes IEEE 802.11i

Eduardo Ferreira de Souza, Paulo André da S. Gonçalves

Centro de Informática - Universidade Federal de Pernambuco (UFPE)
Caixa Postal 7851 – 50.732-970 – Recife – PE – Brasil

{efs,pasg}@cin.ufpe.br

Abstract. *In networks based on the IEEE 802.11i security protocol, the key components of the Pairwise Transient Key (PTK) allow network clients to exchange messages with the appropriate encryption and integrity checking. Due to its importance, the PTK should be kept in secret by the protocol. However, IEEE 802.11i, when not using the IEEE 802.1X standard, is flawed in its process of 4-Way Handshake. It is possible that malicious entities who possess the PSK (Pre-Shared Key) of the network to reproduce the derivation of PTK keys of all authentic clients. In this paper, we propose a mechanism for protection of Nonces, based on the Discrete Logarithm Problem, which aims not to allow that the derivation process of PTK may be reproduced by any malicious entity.*

Resumo. *Em redes baseadas no protocolo de segurança IEEE 802.11i, as chaves que compõem a Pairwise Transient Key (PTK) permitem que os clientes da rede possam trocar mensagens com a devida criptografia e verificação de integridade. Devido a sua importância, a PTK deve ser mantida em completo sigilo pelo protocolo. Porém, o IEEE 802.11i, quando não utiliza o padrão IEEE 802.1X, é falho durante seu processo de 4-Way Handshake. Nele é possível que indivíduos maliciosos que possuam a PSK (Pre-Shared Key) da rede possam reproduzir a derivação de chaves PTK de todos os clientes autênticos. Este artigo apresenta um mecanismo de proteção de Nonces, com base no Problema do Logaritmo Discreto, que tem por objetivo impossibilitar que o processo de derivação da PTK possa ser reproduzido por alguma entidade maliciosa.*

1. Introdução

Atualmente, a segurança das redes sem fio protegidas pelo protocolo IEEE 802.11i tem gerado grande interesse de pesquisa devido à crescente adoção deste protocolo. Como peça fundamental da maioria dos protocolos de segurança, as chaves são as ferramentas que prezam por garantir confidência e integridade às mensagens trocadas entre os clientes autênticos da rede. Elas tem por objetivo impossibilitar que entidades maliciosas possam ter acesso às informações que trafegam.

Os protocolos WPA (*Wi-Fi Protected Access*) [Alliance 2003] e IEEE 802.11i (ou WPA2) [IEEE 2004b] definem uma estrutura de chaves temporais, de forma que as chaves são modificadas automaticamente com certo período de tempo, definido pelo administrador da rede. Pela importância de tais chaves, os protocolos de segurança devem assegurar que elas sejam mantidas em sigilo, garantindo que apenas o cliente e o ponto de acesso as possuam. As chaves temporárias do protocolo IEEE 802.11i, como as chaves de cifragem

e integridade de dados, compõem a *Pairwise Transient Key* (PTK), que é obtida durante o processo de autenticação do cliente na rede. Esse processo ocorre de maneira semelhante nos protocolos WPA e WPA2.

Durante o procedimento de autenticação são trocadas mensagens entre o cliente e o ponto de acesso (*4-Way Handshake*) para garantir que a PTK derivada entre as duas entidades seja a mesma. O protocolo IEEE 802.11i não oferece proteção aos quadros de controle e gerenciamento da rede [Liu and Yu 2006], mas apenas os quadros de dados. Deste modo, as mensagens trocadas durante a etapa de derivação da PTK são passadas em texto-claro.

A posse das informações trocadas durante a autenticação dos clientes da rede torna possível a uma entidade maliciosa, também pertencente à rede, derivar as chaves PTK utilizadas por tais clientes. Desta forma, a entidade maliciosa pode decifrar o conteúdo dos quadros de dados enviados ou recebidos por esses clientes. Este artigo apresenta um mecanismo de proteção do processo de derivação das chaves PTK pelas entidades comunicantes, visando garantir que nenhuma informação que possa comprometer a segurança da rede trafegue em claro.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados à abordagem utlizada; a Seção 3 apresenta os conceitos básicos relativos ao processo de autenticação no protocolo IEEE 802.11i; a Seção 4 descreve o funcionamento do mecanismo de derivação de chaves PTK entre os clientes da rede e o ponto de acesso; a Seção 5 propõe um modelo genérico para assegurar que o processo de derivação de chaves PTK não possa ser reproduzido por entidades maliciosas; a Seção 6 apresenta o protocolo Diffie-Hellman, baseando-se no problema do logaritmo discreto, para derivação de chaves entre duas entidades; a Seção 7 descreve o modelo proposto neste trabalho, com base no modelo apresentado na Seção 5; a Seção 8 analisa a solução proposta neste artigo e avalia a viabilidade de sua implementação; e por fim, a Seção 9 apresenta as conclusões deste trabalho.

2. Trabalhos Relacionados

As principais vulnerabilidades conhecidas na literatura à respeito do *4-Way Handshake* referem-se à segurança do protocolo nos aspectos relacionados à derivação indevida da PTK por entidades maliciosas e à possibilidade de ocorrerem ataques de negação de serviços durante sua troca de mensagens.

Os problemas de negação de serviço são provenientes de ataques de injeção de mensagens indevidas durante o *Handshake*. Deste modo, é possível impedir que a PTK possa ser derivada corretamente pelas entidades autênticas. Esta vulnerabilidade é abordada na literatura através de propostas de modificações do *4-Way Handshake* visando permitir que o processo de derivação ocorra normalmente, independentemente da presença de adversários [He and Mitchell 2005, Rango et al. 2006]. Apesar de ser um problema relevante a ser resolvido, este não compromete diretamente a segurança da rede. No entanto, a possibilidade da derivação indevida da PTK por entidades maliciosas é um problema que além de comprometer a segurança dos clientes da rede, é, até onde se sabe, uma questão ainda não abordada na literatura.

3. Autenticação no Protocolo IEEE 802.11i

O protocolo IEEE 802.11i possui seu mecanismo de autenticação baseado, tradicionalmente, na arquitetura 802.1X, que permite autenticação mútua entre o cliente e o ponto de acesso da rede [IEEE 2004a]. A arquitetura 802.1X é baseada em três entidades comunicantes: O *cliente*, que é o usuário que deseja se conectar a rede; o *ponto de acesso*, que age como um intermediário entre o cliente e os serviços providos pela rede; e o *servidor de autenticação*, que é responsável por verificar as credenciais do cliente, bem como informar sua autenticidade.

Alternativamente ao método de autenticação baseado no padrão 802.1X, o protocolo IEEE 802.11i permite a utilização de um mecanismo baseado em chaves pré-compartilhadas (*Pre-Shared Key* – PSK) entre os clientes da rede e ponto de acesso. Em geral, este método de autenticação é utilizado em redes de pequeno e médio porte, como redes SOHO (*Small Office/Home Office*), onde não se dispõe da infra-estrutura de um servidor de autenticação dedicado.

Uma das grandes vantagens do protocolo IEEE 802.11i está na sua estruturação hierárquica de chaves, que permite a implantação de chaves temporárias visando prover mais segurança à rede. No método de autenticação baseado no padrão 802.1X, após a verificação da autenticidade do cliente, o servidor de autenticação envia ao ponto de acesso e ao cliente uma *Master Session Key* (MSK) [IEEE 2004a]. A partir dessa etapa, apenas o cliente e o ponto de acesso participam do processo de autenticação. A MSK permite que o cliente e o ponto de acesso derivem a *Pairwise Master Key* (PMK), que será a chave-mestra para a derivação das chaves temporárias a serem utilizadas pelo cliente.

No modo WPA/WPA2-PSK, que não faz uso da arquitetura 802.1X, a chave PMK é adotada como sendo a própria PSK da rede, ou seja, todos os clientes da rede possuem a mesma chave-mestra para derivação das chaves temporárias. A partir da obtenção da PMK pelo cliente e pelo ponto de acesso, inicia-se o processo de troca das mensagens (*4-Way Handshake*) entre as entidades para que possam ser derivadas as chaves temporárias. Tal processo acontece de maneira semelhante em ambas as formas de autenticação do protocolo IEEE 802.11i [IEEE 2004a, IEEE 2004b].

4. 4-Way Handshake

O processo de *4-Way Handshake* permite que seja confirmado se houve o compartilhamento de forma correta da chave PMK pelas entidades comunicantes, assim como possibilita ser derivado o conjunto de chaves temporárias *Pairwise Transient Key* (PTK), utilizado durante a troca de mensagens ulterior. A PTK consiste em chaves que serão utilizadas temporariamente para prover a segurança da rede em aspectos como sigilo e integridade dos dados, e, posteriormente, são descartadas durante a comunicação. Após as chaves que compõem a PTK serem descartadas, inicia-se um novo processo de derivação de chaves entre o cliente e o ponto de acesso, a partir da PMK.

O *4-Way Handshake* consiste na troca de quatro mensagens entre o cliente (S) e o ponto de acesso (A), como descrito a seguir: SA, AA, $SNonce$ e $ANonce$ representam os endereços MAC e Nonces do cliente e ponto de acesso, respectivamente; os campos msg_x representam os tipos de mensagem, onde x é o índice de cada mensagem e os campos SN e $SN + 1$ são seus números de seqüência; MIC_{PTK} consiste no *Message*

Integrity Code (MIC) da mensagem enviada, calculado em relação à chave PTK gerada [He and Mitchell 2005]. As quatro mensagens trocadas durante o *4-Way Handshake* são mostradas na Figura 1.

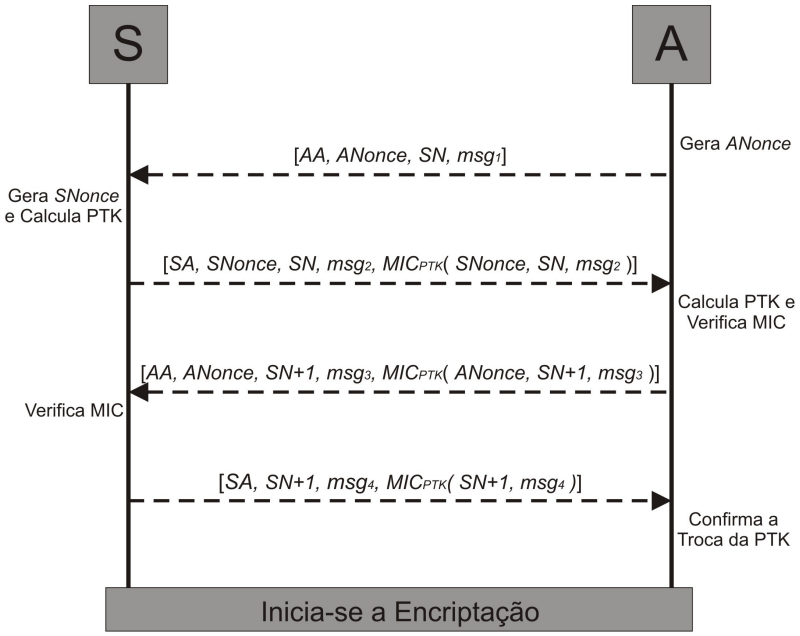

Figura 1. *4-Way Handshake*

O cliente e o ponto de acesso derivam a PTK através de uma função pseudo-aleatória (*Pseudo Random Function* – PRF), onde PTK = PRF (PMK, $AA||SA||ANonce||SNonce$) [He 2004]. Ao receber o primeiro quadro, o cliente possui todos os parâmetros necessários para a derivação da PTK, permitindo-lhe gerar o MIC_{PTK}, que é enviado ao ponto de acesso como parte do segundo quadro. Após o recebimento do segundo quadro, o ponto de acesso calcula a PTK e confirma a autenticação do cliente através da verificação do MIC_{PTK} recebido. O recebimento do terceiro quadro permite que o cliente autentique o ponto de acesso, através da verificação de seu MIC_{PTK}. O quarto quadro é uma confirmação ao ponto de acesso de que a autenticação foi concluída com sucesso, permitindo que ambos possam iniciar o processo de cifragem dos dados.

O objetivo dos Nonces gerados pelo cliente e pelo ponto de acesso é permitir que cada nova PTK gerada seja diferente das chaves já derivadas anteriormente. Para que a PTK se modifique a cada *Handshake*, é necessário que os parâmetros da função PRF se modifiquem, ou seja, pelo menos uma das entradas da função deve ser alterada para que uma nova PTK seja gerada a cada derivação. Dentre os parâmetros da função PRF, apenas os Nonces variam a cada *Handshake*, pois são gerados de forma aleatória pelas entidades comunicantes.

4.1. Vulnerabilidade Durante o *4-Way Handshake*

O processo de derivação de chaves ocorre sem que chaves sejam transmitidas pelo canal de comunicação entre o cliente e o ponto de acesso. Através das mensagens trocadas durante o *4-Way Handshake*, ambas as entidades possuem todas as informações necessárias

para a derivação da mesma PTK. O problema de segurança referente ao *4-Way Handshake* não está diretamente relacionado com a forma como a PTK é derivada, mas com o fato que o processo de derivação de chaves pode simplesmente ser reproduzido [Fogie 2005]. Isto decorre do fato de que todas as mensagens que trafegam pelo canal de comunicação podem ser capturadas escutando-se o canal durante a autenticação, já que estas trafegam em texto-claro.

Para que a derivação da PTK possa ser reproduzida por entidades não participantes do processo, tais entidades precisam conhecer todos os parâmetros da função PRF, ou seja, os endereços e Nonces do cliente e do ponto de acesso, bem como a PMK. Porém, durante a troca de todas as mensagens, os endereços MAC das entidades trafegam em claro e, de forma semelhante, as três primeiras mensagens trocadas possuem os Nonces do cliente e do ponto de acesso passando em claro. Com tais informações, uma entidade maliciosa que tente derivar as chaves PTK dos clientes da rede apenas precisará descobrir a PMK, para que possa reproduzir o resultado da função PRF.

Considerando ambientes onde não haja um servidor de autenticação, ou seja, onde a PMK é a própria PSK, é plausível e deve ser considerado o caso onde algum dos clientes autênticos à própria rede seja uma entidade maliciosa que vise obter as chaves PTK utilizadas pelos outros clientes. Em tal situação a rede apresenta-se totalmente vulnerável, pois um possível usuário malicioso terá acesso a todas as informações necessárias para reproduzir o processo de derivação de chaves dos clientes da rede, já que tal indivíduo possui a chave PSK da rede.

Para ambientes que utilizam a arquitetura 802.1X, a rede encontra-se protegida contra tal tipo de ataque, pois fica inviável para um usuário mal intencionado conseguir obter as chaves da rede. Neste caso, um cliente conhece apenas as próprias credenciais, de forma que cada cliente derivará uma PMK diferente durante o processo de autenticação. A utilização de um servidor de autenticação se mostra eficiente com relação a esse tipo de ataque, porém nem sempre o ambiente em que a rede está sendo implantada disponibiliza tal infra-estrutura, como é o caso da maioria das redes domésticas e das pequenas empresas.

5. Método para Prover Segurança Durante o *4-Way Handshake*

A solução proposta neste artigo consiste em um mecanismo de proteção para o *Handshake* de forma que, caso um usuário malicioso possua a PSK, ele esteja impossibilitado de conhecer efetivamente as chaves PTK utilizadas pelos clientes, mesmo que os dados que trafegam na rede durante o processo de derivação de chaves sejam interceptados.

Além da circunstância onde o adversário é um cliente da rede, ainda existe a possibilidade da PSK ser uma chave fraca e se mostrar vulnerável a ataques de dicionário [He and Mitchell 2005]. Neste caso, é possível para qualquer adversário realizar uma busca exaustiva sobre possíveis chaves, visando sua obtenção. Vale ressaltar que o objetivo desse artigo não está em propor técnicas para a obtenção da PSK, mas sim propor um mecanismo de proteção para a rede, dado que o adversário já possui tal chave.

Dentre os parâmetros aplicados à função PRF, os endereços e os Nonces trafegam em claro durante o *4-Way Handshake*, porém destes, os endereços MAC são passados em texto-claro durante outras etapas na comunicação das entidades da rede, de forma

que não faz sentido proteger tais dados durante o processo. No entanto os Nonces são utilizados exclusivamente durante o processo de *Handshake*, não sendo usados novamente durante nenhuma etapa da comunicação entre as entidades. Mesmo que ocorram outros *Handshakes* entre o cliente e o ponto de acesso, os Nonces não se repetirão, pois nesse caso serão gerados novos Nonces pelas entidades comunicantes. Esse fato justifica a necessidade de proteção dos Nonces para que os parâmetros utilizados pela função PRF sejam protegidos garantidamente. A insegurança em se trafegar os Nonces em claro na rede decorre do fato de que estes foram criados apenas para permitir que diferentes chaves fossem geradas a cada derivação.

Antes das mensagens utilizadas na derivação da PTK serem derivadas entre o cliente e o ponto de acesso, é proposto que uma nova chave seja derivada entre as duas entidades comunicantes com a finalidade de cifrar os Nonces durante o *Handshake*. Este artigo propõe que a derivação da chave para proteção dos Nonces seja baseada no Problema do Logaritmo Discreto, abordagem utilizada em [Diffie and Hellman 1976, Gamal 1985].

6. Problema do Logaritmo Discreto e o Protocolo Diffie-Hellman

O problema do logaritmo discreto é aplicado a grupos cíclicos, ou seja, grupos que podem ser gerados por um único elemento [Diffie and Hellman 1976]. Dado um grupo cíclico G e dois elementos g e y pertencentes a G, o Problema do Logaritmo Discreto consiste em encontrar um inteiro x, tal que $y = g^x$, ou seja, encontrar o $\log_g y$. Assumindo que p é um número primo que representa ordem do grupo, tem-se que $\log_g y \equiv x \ (mod\ p)$.

Baseando-se na dificuldade de resolver o problema do logaritmo discreto, que se encontra na classe de problemas NP, Diffie e Hellman [Diffie and Hellman 1976] propuseram um algoritmo de derivação de chaves criptográficas entre duas entidades E_1 e E_2, que é descrito da seguinte forma:

1. Um número primo p é tornado público, bem como um valor g, gerador do grupo cíclico em questão;
2. E_1 escolhe um valor inteiro x_1 e computa $y_1 = g^{x_1} \ (mod\ p)$. Em seguida E_1 envia y_1 para E_2;
3. E_2 escolhe um valor inteiro x_2 e computa $y_2 = g^{x_2} \ (mod\ p)$. Em seguida E_2 envia y_2 para E_1;
4. E_1 computa a chave compartilhada como sendo $k_1 = y_2^{x_1} \ (mod\ p)$;
5. E_2 computa a chave compartilhada como sendo $k_2 = y_1^{x_2} \ (mod\ p)$.

Os valores de k_1 e k_2 são os mesmos e ambos iguais a $g^{x_1 . x_2} \ (mod\ p)$. A grande vantagem de tal método é o fato de que as mensagens podem ser trocadas em um canal inseguro, porém a chave derivada pelo processo é segura [Jonathan Katz 2007]. Um adversário que escute o tráfego do canal de comunicação estará impossibilitado de descobrir o valor da chave k, pois se faz necessário o conhecimento de, ao menos, o valor de x_1 ou x_2 para que possa ser realizada a derivação da chave com sucesso.

Algumas considerações devem ser feitas a respeito dos valores x_1, x_2, g e p para que o mecanismo de derivação de chaves possa ser considerado difícil de ser invertido, em relação a sua complexidade computacional. As variáveis devem ser inteiros grandes, preferencialmente maiores que 1024 bits, além de que $(p–1)/2$ também deve ser um número

primo. Os valores de x_1 e x_2 devem pertencer ao grupo cíclico, ou seja, devem ser inteiros menores que p. O inteiro g deve ser um gerador do grupo e deve ser uma raiz primitiva do módulo p, de forma que a ordem multiplicativa de g $(mod\ p)$ deve ser $\phi(n)$, onde ϕ é a função totiente [Lehmer 1932].

Como o protocolo Diffie-Hellman baseia-se na dificuldade de resolver o Problema do Logaritmo Discreto, que é um problema da classe NP, a dificuldade de se obter a chave K apenas escutando-se o canal de comunicação durante a troca de mensagens entre as entidades comunicantes é equivalente à dificuldade de se descobrir um algoritmo que resolva em tempo polinomial qualquer instância do Problema do Logaritmo Discreto. Atualmente, os melhores algoritmos conhecidos na literatura para resolver o Problema do Logaritmo Discreto são variações do método descrito em [Pollard 1978], e executam em tempo exponencial de O($\sqrt{n}$), onde n é a ordem do grupo [Koblitz and Menezes 2004].

7. O Protocolo Proposto

A proposta deste artigo está em um novo mecanismo de troca de mensagens para derivação de chaves PTK no protocolo IEEE 802.11i, nomeado de *6-Way Handshake*. Este mecanismo é proposto visando substituir o *4-Way Handshake*, modelo utilizado até então. O *6-Way Handshake* tem por objetivo proteger as chaves PTK da rede durante o seu processo de derivação, para que estas não possam ser reproduzidas por entidades maliciosas. Tal proteção é provida através da cifragem dos Nonces durante o *Handshake*.

Para proteger os valores dos Nonces, são trocadas duas mensagens entre o cliente e ponto de acesso, de forma a permitir que ambos derivem uma chave K e realizem uma operação de *ou exclusivo* bit-a-bit entre K e o *Nonce* a ser enviado. Os processos de cifragem e decifragem dos Nonces, obtidos através da operação de *ou exclusivo*, serão os únicos momentos em que a chave K será útil à comunicação entre as entidades, podendo ser descartada após o *6-Way Handshake*.

O *6-Way Handshake* consiste na troca de seis mensagens entre o cliente (S) e o ponto de acesso (A), das quais as duas primeiras possuem a finalidade de estabelecer uma chave compartilhada K para proteção dos Nonces e as quatro mensagens subjacentes visam à derivação da PTK. Os valores p e g são respectivamente a ordem e o gerador do grupo cíclico utilizado para derivar K; SA , AA, $SNonce$ e $ANonce$ são os endereços MAC e Nonces do cliente e do ponto de acesso; ANK e SNK representam respectivamente os valores cifrados, através da chave K, dos campos $ANonce$ e $SNonce$; os campos msg_x representam os tipos de mensagem, onde x é o número da mensagem em questão e $SN, SN + 1$ e $SN + 2$ são seus números de seqüência; MIC_{PTK} consiste no MIC da mensagem enviada, calculado com base na chave PTK derivada.

Inicialmente o ponto de acesso define os valores de p e g, respeitando os requisitos necessários, como já descritos, para que o esquema seja considerado seguro. Ao construir um método baseado em Logaritmo Discreto, o tamanho das variáveis deve ser da ordem de 1024 bits, com base nas limitações computacionais atuais. Os valores de y_1 e y_2 a serem computados pelas entidades comunicantes ocorrem de forma semelhante ao mecanismo proposto por Diffie e Hellman, bem como o cálculo da chave K. O protocolo proposto é mostrado detalhadamente através da Figura 2.

A derivação da chave PTK no *6-Way Handshake* ocorre de forma semelhante ao *4-Way Handshake*, de maneira que tal chave é obtida a partir da função pseudo-aleatória

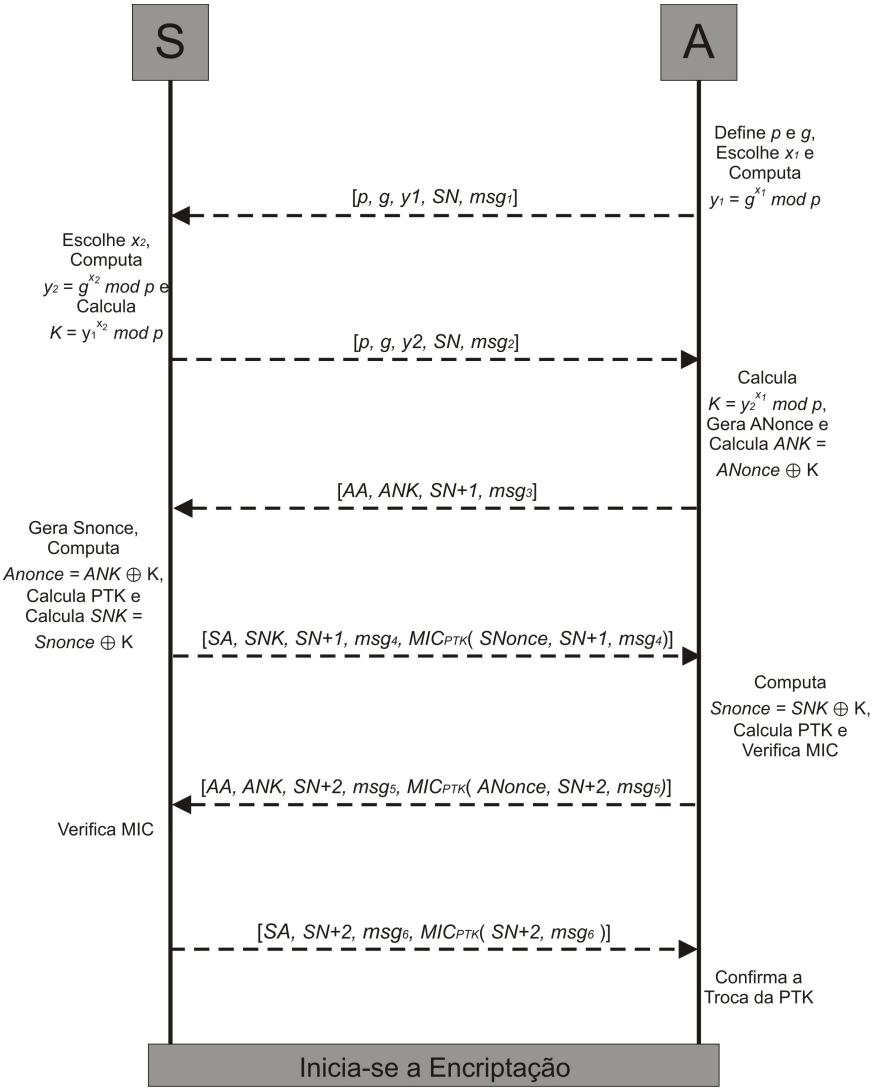

Figura 2. Modelo Proposto – *6-Way Handshake*

PRF, onde PTK = PRF (PMK, $AA||SA||ANonce||SNonce$). No entanto, ambas as entidades devem computar uma operação de *ou exclusivo*o entre o $Nonce$ cifrado (ANK e SNK) e a chave K para obter o valor plano do $Nonce$ contido na mensagem recebida, para que tal valor possa ser aplicado como parâmetro à função PRF.

8. Avaliação

Diante das funções algébricas adicionadas ao sistema através do protocolo Diffie-Hellman, se faz necessário que haja viabilidade computacional para a implementação do mecanismo proposto. Atualmente existem diversas abordagens de implementações do protocolo Diffie-Hellman, tanto em *software* quanto em *hardware*, que visam analisar sua eficiência até mesmo em dispositivos com capacidade de processamento limitada.

Em [Shihab and Langhammer 2003] é utilizada uma abordagem de implementação do protocolo Diffie-Hellman em dispositivos FPGA (*Field Programmable Gate Array*), com o auxílio do algoritmo Montgomery [Montgomery 1985], usado para reduzir o custo computacional do sistema na realização de multiplicações e

exponenciações modulares. Em tal abordagem foram utilizados expoentes e módulos de 1024 bits para os grupos cíclicos avaliados. Conseguiu-se obter uma taxa de até 640 trocas de chaves por segundo, dependendo do dispositivo FPGA usado. Isto demonstra que o custo computacional adicionado ao sistema através do protocolo Diffie-Hellman é pouco, tornando completamente viável a implementação do *6-Way Handshake* nos diversos dispositivos que utilizam o padrão IEEE 802.11i.

O processo de obtenção da chave de cifragem dos $Nonces$ considerado neste artigo pode ser adaptado para um mecanismo baseado no Problema do Logaritmo Discreto em Curvas Elípticas. Esta abordagem, com base na proposta de Koblitz e Miller [Koblitz 1987, Miller 1986], poderia reduzir substancialmente necessidade de se utilizar variáveis com valores elevados para que o grupo cíclico em questão seja considerado seguro. Existem estudos que afirmam que há uma equivalência entre os graus de segurança providos por um mecanismo baseado em logaritmo discreto com 1024 bits e uma mesma abordagem baseada em curvas elípticas com 160 bits [Saeki 1997, Odlyzko 2000].

9. Conclusão

Este artigo apresentou um mecanismo de troca de mensagens, nomeado de *6-Way Handshake*, para derivação segura da PTK no protocolo IEEE 802.11i. Foi utilizada uma abordagem baseada no Problema do Logaritmo Discreto e no protocolo Diffie-Hellman, visando proteger os Nonces que trafegam entre o cliente e o ponto de acesso durante a etapa de autenticação.

O *6-Way Handshake* se mostra como uma solução viável ao problema de derivação indevida da PTK. O custo computacional adicionado à etapa de autenticação é baixo, visto que a utilização do protocolo Diffie-Hellman na implementação do mecanismo não acrescenta cálculos de expressivos esforços computacionais ao sistema. Além de que, o *6-Way Handshake* apenas supera em duas mensagens a quantidade de quadros trocados entre as entidades comunicantes, em relação ao *4-Way Handshake*.

Referências

Alliance, W. F. (2003). Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks.

Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography. In *Proceedings of IEEE Transactions on Information Theory*, volume 22, pages 644–654.

Fogie, S. (2005). Cracking Wi-Fi Protected Access (WPA), Part 2. `http://www.fermentas.com/techinfo/nucleicacids/maplambda.htm`.

Gamal, T. E. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, volume 31, pages 10–18, Santa Barbara, USA.

He, C. (2004). Analysis of the 802.11i 4-Way Handshake. In *Proceedings of ACM Workshop on Wireless Security*, pages 43–50, Philadelphia, PA, USA. ACM Press.

He, C. and Mitchell, J. C. (2005). Security Analysis and Improvements for IEEE 802.11i. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, pages 90–110.

IEEE (2004a). IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control.

IEEE (2004b). Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security.

Jonathan Katz, Y. L. (2007). *Introduction to Modern Cryptography*. Chapman & Hall/CRC.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. In *Proceedings of Mathematics of Computation*, volume 48, pages 203–209.

Koblitz, N. and Menezes, A. J. (2004). A Survey of Public-Key Cryptosystems. *SIAM Rev.*, 46:599–634.

Lehmer, D. H. (1932). On Euler's Totient Function. *Bulletin of the American Mathematical Society*, (38):27–36.

Liu, C. and Yu, J. (2006). An Analysis of DoS Attacks on Wireless LAN. In *Proceedings of International Conferences on Wireless Networks and Emerging Technologies*, Canada.

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. In *Proceedings of Advances in Cryptology–CRYPTO '85*, pages 417–426. Springer-Verlag.

Montgomery, P. L. (1985). Modular Multiplication Without Trial Division. In *Proceedings of Mathematics of Computation*, volume 44, pages 519–521.

Odlyzko, A. (2000). Discrete logarithms: The past and the future. *Designs, Codes, and Cryptography*, 19:129–145.

Pollard, J. M. (1978). Monte Carlo Methods for Index Computation (mod p). In *Proceedings of Mathematics of Computation*, volume 32, pages 918–924.

Rango, F. D., Lentini, D. C., and Marano, S. (2006). Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i. *EURASIP Journal on Wireless Communications and Networking*.

Saeki, M. (1997). Elliptic Curve Cryptosystems. Master's thesis, School of Computer Science, McGill University.

Shihab, A. and Langhammer, M. (2003). Implementing IKE Capabilities in FPGA Designs. `http://www.eetimes.com/story/OEG20031205S0005`.