Um Controle de Autenticação de Handover Vertical para Prevenir Ataque de Repetição em Redes Heterogêneas Sem Fio

Adi Marcondes[1], **Michele Nogueira**[1], **Aldri Santos**[1]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR
Caixa Postal 19.081 – 81.531.980 – Curitiba – PR – Brasil

{an.marcondes, michele,aldri}@inf.ufpr.br

Abstract. *The wireless heterogeneous networks allows increased compliance data transmission, as they consider interoperability in differents networks technologies. Moreover, the authentication service supports interoperability and admits access control in the devices. In the literature, several authentication schemes have been proposed for security this service during the transition in networks, but these schemes do not prevent effectively replay attack. Thus, this paper proposes the authentication scheme CAH to prevent replay attack in heterogeneous networks. The scheme consists of a unified authentication between different network technologies using the matching method and the uniqueness of message verification in transition networks. The mechanism checks the time and amount of messages, and sends information of the mobile devices to other networks via the overlay. The evaluation of this scheme compares the results with the UHA scheme using metrics of safety and performance.*

Resumo. *As redes heterogêneas sem fio possibilitam uma maior abrangência à transmissão de dados, visto que elas consideram a interoperabilidade em redes de tecnologias diferentes. Para isso, o serviço de autenticação oferece suporte à interoperabilidade e permite o controle de acesso dos dispositivos nas redes. Na literatura, vários esquemas de autenticação foram propostos para a segurança deste serviço durante a transição nas redes, porém estes esquemas não previnem o ataque de repetição de maneira eficaz. Diante disso, este trabalho propõe o esquema de autenticação CAH para prevenir o ataque de repetição em redes heterogêneas. O esquema consiste de uma autenticação unificada entre redes de tecnologias diferentes utilizando o método de pareamento e a verificação da unicidade das mensagens na transição de redes. O mecanismo verifica o tempo e a quantidade de mensagens, e envia informações dos dispositivos móveis para outras redes através da sobreposição. A avaliação deste esquema compara os resultados com o esquema UHA usando métricas de segurança e desempenho.*

1. Introdução

As redes heterogêneas sem fio (HetNets) abrangem várias tecnologias de redes e permitem que os usuários portadores de dispositivos computacionais móveis trafeguem por diferentes áreas de transmissão [Damnjanovic et al. 2011]. Deste modo, a proliferação destes dispositivos resultou no aumento intensivo do fluxo de dados que possui o suporte da interoperabilidade nas redes [Ranjan et al. 2014]. A interoperabilidade representa um requisito das HetNets para conectividade e sustentação dos serviços usados pelos usuários.

O *handover* vertical consiste de um processo da rede para a interoperabilidade que efetua a transferência da conexão [Xenakis et al. 2014]. Contudo, a execução do processo de *handover* vertical nas redes necessita de um serviço essencial chamado de autenticação.

A autenticação baseia-se em um serviço que auxilia os sistemas computacionais no reconhecimento dos usuários [Kent et al. 2015]. Este serviço lida com a segurança e o controle de acesso dos dispositivos móveis nas redes [Sandhu and Samarati 1994]. Apesar disso, o serviço de autenticação está sujeito a problemas de desempenho e segurança quando existe a necessidade do dispositivo móvel efetuar o *handover* vertical [He et al. 2015]. Os problemas do serviço de autenticação acarretam no aumento do custo de processamento dos dispositivos móveis e na descontinuidade ou atraso dos serviços usados pelos usuários das redes sem fio. Além dos prejuízos no desempenho, a ausência de confidencialidade na comunicação dos dispositivos móveis e da rede resultam em ataques que visam o acesso não autorizado e a perda de conexão afetando a disponibilidade dos serviços. Alguns ataques de autenticação tem como característica a obtenção dos quadros de transmissão durante a associação dos dispositivos móveis nas redes heterogêneas. Um dos principais ataques, chamado de ataque de repetição, representa a captura e replicação dos quadros de transmissão na comunicação das entidades das redes. Este ataque, nas redes heterogêneas, tem como meta o acesso não autorizado em um ponto de acesso através os quadros de autenticação dos dispositivos móveis legítimos obtidos durante o *handover* vertical.

Várias abordagens na literatura buscam resolver os problemas no serviço de autenticação que envolvem a segurança e o desempenho. Algumas soluções de autenticação têm como base a identidade dos dispositivos móveis [Cao et al. 2012, Feng and Jiao 2012, Li et al. 2012]. Outras soluções utilizam a distribuição da autenticação [Cheng et al. 2014] e formação de grupos de entidades [Fu et al. 2013] para proteger a rede contra o acesso não autorizado sem afetar o desempenho dos serviços de rede. No entanto, estas estratégias não garantem a segurança do serviço de autenticação no contexto de HetNets em razão de não considerarem as diferentes características de transmissão de dados [Cao et al. 2014]. Com intuito de melhorar o desempenho, algumas abordagens utilizam a criptografia baseada em pareamento na geração de identidades [He et al. 2012] para otimizar o tempo de execução da autenticação no serviço de *handover*. Na tentativa de melhorar o desempenho do processo de autenticação, estas soluções apresentam vulnerabilidades na transição entre as redes heterogêneas.

Os métodos de segurança utilizados na proteção da autenticação fundamentam-se no tempo de transmissão dos quadros e requisição de conexão entre o dispositivo móvel e o ponto de acesso da rede [Yu et al. 2013]. No entanto, o tempo de transmissão dos quadros assume apenas redes homogêneas, ou seja, com características de transmissão semelhantes [Hu et al. 2003]. Logo, a integração dos esquemas de autenticação nas HetNets oferece uma solução mais robusta contra o ataque de repetição. Ademais, métodos como a validação dos quadros de transmissão recebidos pelas redes e a distribuição de autenticação dos dispositivos entre as entidades autenticadoras anulam o acesso indevido.

Este trabalho apresenta o controle de autenticação de *handover* (CAH) que possui o objetivo de prevenir o ataque de repetição na autenticação do serviço de *handover* vertical dos dispositivos móveis nas redes heterogêneas. O CAH compreende duas fases de autenticação que envolvem os dispositivos móveis e as redes heterogêneas, e um me-

canismo de proteção que analisa os quadros de transmissão dos dispositivos móveis. Para avaliar o controle de autenticação CAH foram utilizadas métricas de segurança e de desempenho. Além disso, os resultados foram comparados com o esquema de autenticação UHA. As simulações mostram que o CAH dispõem de uma segurança mais eficaz contra o ataque de repetição nas HetNets e um melhor desempenho do serviço de autenticação no *handover* vertical.

O artigo está organizado desta forma: a Seção 2 apresenta os trabalhos relacionados. A Seção 3 detalha o funcionamento do controle de autenticação proposto. A Seção 4 mostra a avaliação de segurança e desempenho do esquema. Finalmente, a Seção 5 apresenta as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Os esquemas de autenticação com base na identidade utilizam as informações de identificação dos dispositivos móveis para autorizar o acesso à rede. O esquema UHA [Cao et al. 2012] sucede inicialmente da autenticação do dispositivo móvel através da rede de maior sobreposição de transmissão sem fio, onde existe uma entidade que cria as identidades e chaves dos dispositivos móveis. Apesar disso, os quadros de transmissão continuam vulneráveis e ocorrem atrasos no processo de autenticação do serviço de *handover* nas redes. O trabalho WAPI [Feng and Jiao 2012] se baseia na identidade e usa o protocolo de combinação lógica (PCL) [Cremers 2008]. Entretanto, este trabalho não oferece segurança contra ataques de quadros de transmissão na comunicação das entidades das redes. O esquema de autenticação LRA [Li et al. 2012] propôs uma autenticação para o serviço de *handover* com a pretensão de reduzir o processamento computacional e prover o anonimato para os dispositivos móveis sem a necessidade de um servidor de autenticação residencial. A prevenção dos ataques que usam os quadros de transmissão falha em razão da metodologia de validação da transmissão permitir quadros repetidos.

O trabalho DDA [Cheng et al. 2014] consiste de uma abordagem de autenticação distribuída. Este controle de autenticação tem como prioridade o anonimato e a distribuição da autenticação para solucionar os problemas de segurança e desempenho nas redes. Através do reconhecimento de dispositivos móveis e pontos de acessos como membros de um grupo, os algoritmos de assinatura adotados nesta abordagem fornecem a verificação de identidade. Os dispositivos móveis assinam as mensagens em nome deste grupo para se autenticar nas redes. Isto oferece uma resistência aos ataques que visam o anonimato e a ausência da disponibilidade. Esta estratégia não inviabiliza o ataque de repetição quando existe uma rede maliciosa que obtém informações de um dispositivo móvel e assim utilizadas para acesso em outra rede.

O controle de autenticação GHAP [Fu et al. 2013] estabelece um esquema baseado em grupos de *handover* para os dispositivos móveis. Este controle de autenticação consiste de três fases para desenvolvimento, inicialização e autenticação no handover. Além disso, o GHAP cria um contexto de segurança para os membros do grupo de *handover* para o ponto de acesso da rede destino usando o método SCT (*Security Context Transfer*). Isto acontece durante a fase de autenticação do dispositivo móvel. Este esquema tem o objetivo de resistir contra o ataque dominó existente nos métodos SCT. No entanto, os ataques que visam os quadros de comunicação tem efeitos sobre a autenticação.

O esquema PairHand [He et al. 2012] usa a criptografia baseada em pareamento

para a geração de identidades e chaves. Ademais, o objetivo deste esquema tem o propósito a alta eficiência no desempenho dos serviços da rede. Para isso, o esquema adota pseudônimos para proteger a privacidade e requerem maior capacidade de armazenamento dos dispositivos móveis. Isto possibilita o pré-processamento de um grande conjunto de pseudônimos de autenticação no servidor de gerência central. Apesar disso, a abordagem não considera a sobreposição nas redes heterogêneas para o controle de acesso. Isto permite que ataques de quadros sejam executados.

3. Controle de autenticação

Esta seção apresenta o controle de autenticação proposto CAH para prevenir o ataque de repetição na autenticação durante o processo de *handover* nas redes heterogêneas. Primeiramente apresenta-se o modelo da rede assumido para o controle de autenticação e o modelo de ataque. Em seguida, a especificação do esquema de autenticação que consiste das fases de inicialização e de autenticação, e o mecanismo de proteção são abordados.

3.1. Modelo da rede

As redes heterogêneas agregam diversos dispositivos computacionais que possuem características e funcionalidades diferentes [Heath et al. 2013].No modelo proposto, estes dispositivos computacionais consistem dos nós ou dispositivos móveis dos usuários representados pelo conjunto *N*, dos pontos de acesso (*AP*) e dos autenticadores (*A*). Cada autenticador compreende uma rede que se encontra no conjunto de redes heterogêneas.

A HetNet é composta pelo conjunto de n nós, móveis ou fixos, denotado por *N* = $\{n_1, n_2, n_3, ..., n_i\}$ tal que $n_i \in N$. Estes nós são classificados em nós comuns (*Nc*) e nós atacantes (*Na*), onde *Nc* $\subseteq$ *N*, *Na* $\subseteq$ *N* e *Nc* $\bigcup$ *Na* = *N*. Além disso esses nós possuem relação com os pontos de acesso das redes heterogêneas. Os pontos de acesso são representados por *AP*= $\{ap_1, ap_2, ap_3, ..., ap_i\}$ tal que $ap_i \in AP$, sendo que, o *ap* representa um ponto acesso específico dentro do conjunto de ponto de acesso *AP* em uma rede. Cada rede possui um autenticador (*A*) que realiza a autenticação dos nós. Logo o conjunto de redes heterogêneas (*H*) = $\{A_1, A_2, A_3, ..., A_i\}$.

Um ou mais elementos do conjunto de pontos de acesso *AP* está associado com um elemento do conjunto de autenticadores *A* de tal forma que são denotados por $F : AP \rightarrow A$. Os elementos do conjunto de nós *N* tem relação com elementos dos conjuntos *AP* e *A*. Logo, a relação pode ser representada por $N^{ap,a}$. A comunicação entre os dispositivos móveis e as redes acontece no meio sem fio. A comunicação nas redes heterogêneas ocorre através de um canal seguro, e isto impossibilita ataques na comunicação das entidades das redes (*H*).

3.2. Modelo do ataque

As HetNets estão sujeitas a diversos tipos de ataques que utilizam os quadros de autenticação. Neste trabalho é considerado o ataque de repetição. Neste ataque, os atacantes realizam a captura dos quadros de transmissão da autenticação enviados de um dispositivo móvel para um ponto de acesso. Os quadros capturados podem ser decifrados pelos atacantes e replicados no ponto de acesso. A replicação dos quadros tem como objetivo o acesso não autorizado aos recursos da rede. Para isso, os quadros de replicação devem ser validados por uma entidade autenticadora de uma rede presento no conjunto de redes heterogêneas (*H*).

O dispositivo móvel (*Nc*) efetua uma requisição para se conectar a uma rede com o ponto de acesso (*AP*). Logo, esta requisição no meio sem fio é enviada em formato de quadros de transmissão no qual, o *AP* reconhece a mensagem e envia para o autenticador *A* da rede. Um dispostivo móvel malicioso *Na* executa a captura dos quadros de transmissão da autenticação de *Nc*. Através da captura, o atacante pode replicar os quadros para efetuar uma inconsistência de informações no autenticador *A* e assim obter acesso não autorizado.

O ataque de repetição pode ser executado para atacar o dispositivo móvel. Neste caso, o *Na* replica os quadros de transmissão enviados pelo *AP* para o *Nc* a fim de confundir o dispositivo. Com esta forma de ataque, o atacante simula um *AP* falso para diversas finalidades como roubo de informações e também realizar outros ataques maliciosos. O ataque visando o usuário móvel também pode ser replicado de forma constante para esgotar os recursos limitados do *Nc*.

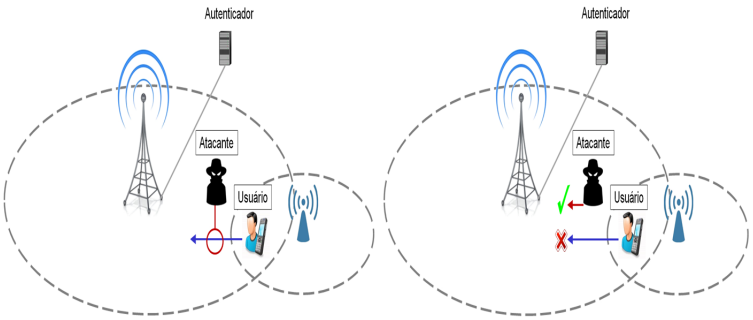

Figura 1. Ataque de repetição

A Figura 1 representa o ataque de repetição. No instante T1, o usuário do dispositivo móvel (UE) efetiva a autenticação durante o processo de *handover* vertical nas redes heterogêneas para obter acesso na rede representada pelo AP2. Um dispositivo malicioso (ATCK) sucede a captura dos quadros de transmissão no alcance do AP2. Logo, o UE, que esta em movimento, se autentica na rede destino e o ATCK efetua a captura. No instante T2, o UE se autentica com a rede de maior transmissão de dados sem fio através do AP1. O ATCK replica os quadros capturados de UE no AP2 e realiza a conexão com a rede para usufruir dos recursos e serviços oferecidos.

3.3. Esquema de autenticação CAH

O esquema de autenticação CAH baseia-se em uma autenticação unificada nas redes heterogêneas, na criptografia de pareamento e no mecanismo de proteção de ataques de repetição dos quadros de transmissão. A autenticação acontece em duas fases que são a inicialização e autenticação. Na fase de inicialização, o dispositivo móvel realiza a primeira autenticação para que a autenticação no serviço de *handover* seja realizada nas HetNets. Na fase de autenticação, o dispositivo móvel efetua a autenticação de *handover* e o mecanismo de proteção previne o ataque de repetição. Neste esquema, o ataque de repetição no serviço de autenticação de *handover* não surte efeito nas redes heterogêneas em virtude do mecanismo de proteção utilizar métodos de verificação tempo, verificação de quantidade de quadros recebidos na rede e informar as redes próximas sobre os dispositivos móveis.

3.3.1. Fase de inicialização

A fase de inicialização tem o objetivo de efetivar uma conexão segura para o usuário do dispositivo móvel. Esta autenticação acontece através de um gerenciador de autenticação central que auxilia o controle de acesso nas redes. O gerenciador central distribuí as identidades e as chaves para os dispositivos computacionais presentes nas redes heterogêneas. Desta forma, o dispositivo ao se autenticar com o gerenciador central ele obtém identidade e chaves que são utilizadas nas demais redes. O autenticador central se encontra no núcleo de processamento da rede de maior abrangência de sinal sem fio. A rede de maior abrangência integra as redes de menor poder de sinal sem fio. A integração de identidades e chaves tem relação com o a criptografia baseada em pareamento.

A Criptografia Baseada em pareamento (*Pairing Based Cryptography*) possibilita uma melhora de desempenho no serviço de transição. O funcionamento compreende de um grupo cíclico aditivo G e um grupo cíclico multiplicativo GT de mesma ordem q. O grupo G é um conjunto que possui as propriedades de identidade e associação. O parâmetro P é um gerador de arbitrário de G e aP que indica o P posicionado para ele mesmo. Um mapeamento bilinear e corresponde à $e = G * G \rightarrow GT$ que satisfaz as regras de bilinearidade e computabilidade. A bilinearidade representa a regra $e(aP, bQ) = e(P, Q)^a b$, onde $P, Q \in G$ e $a, b \in Z * q$. O valor $Z * q$ corresponde à $Z * q = \{\rho | 1 \leq \rho \leq q-1\}$. O mapeamento bilinear deve cumprir a regra $e(P, P) \neq 1$. A regra de computabilidade constitui-se de um algoritmo de eficiência que calcula $e(P, Q)$ para qualquer $P, Q \in G$.

A Figura 2 representa a fase de inicialização. O dispositivo móvel (UE) requisita uma conexão na rede de maior alcance. Primeiramente, o gerenciador central(KGC) efetua a autenticação do dispositivo. Através da autenticação,a identidade para o UE é gerada juntamente com as chaves pública e privada (chave assimétrica) para acesso entre as redes heterogêneas. A partir disso, o UE requisita autenticação na rede de menor alcance para criação de identidade e chaves. Neste caso, esta identidade e chaves devem ser armazenadas no gerenciador central das redes para ser associado a outros tipos de redes. A associação ocorre quando o UE requisitar em outro momento a autenticação com o outro tipo de rede através da relação entre as identidades e chaves.

Seja, G e GT de mesma ordem q e P um gerador randômico de G, $G * G \rightarrow GT$, cria-se um mapa bilinear. Assim, o gerenciador de chave central escolhe um número aleatório $s \in Z * q$ como a chave mestra e calcula a chave pública correspondente $pub = sP$. Além disso, duas funções hash de segurança $H1$ e $H2$ são determinadas, onde $H1 : \{0,1\}* \rightarrow G$ e $H2 : \{0,1\}* \rightarrow Z * q$. O gerenciador central publica os parâmetros de autenticação das redes $\{G, GT, q, P, pub, H1, H2\}$ e mantém a chave privada secretamente. Para cada ponto de acesso, o gerenciador de chaves central calcula $H1(IDAP)$ como a chave pública e $sH1(IDAP)$ como a chave privada. Desta forma, este gerenciador envia as chaves para o ponto de acesso (AP), onde $IDAP$ representa a identidade de cada AP.

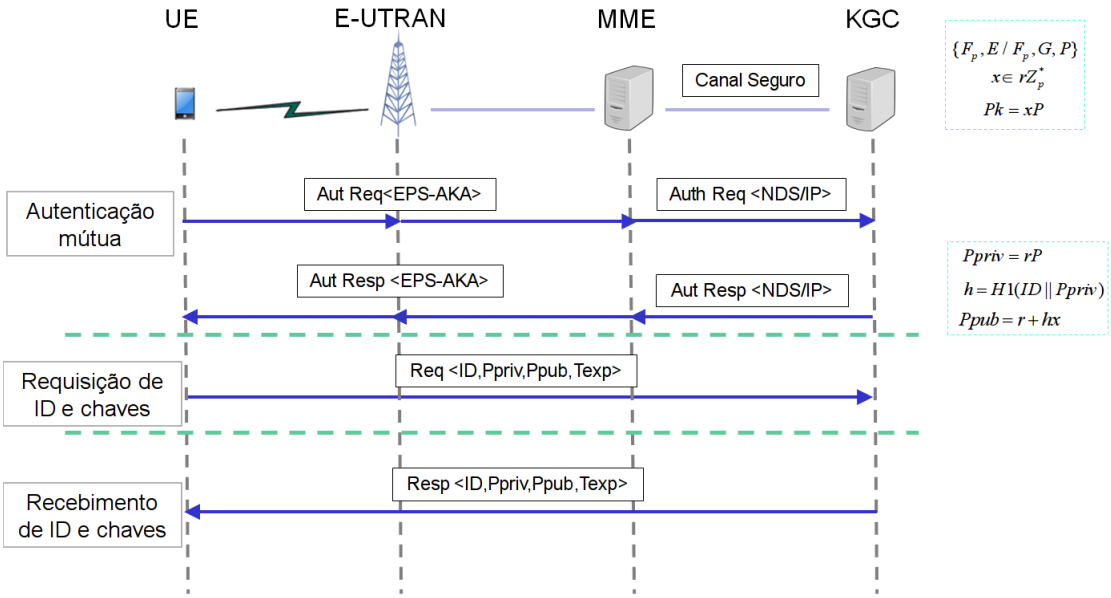

Figura 2. Inicialização

3.3.2. Fase de autenticação

A fase de autenticação no *handover* tem o propósito de prevenir o ataque de repetição durante o *handover* do dispositivo móvel. Nesta fase, o dispositivo móvel utiliza as chaves pública e privada para efetuar a autenticação durante o *handover* vertical entre redes heterogêneas. A chave pública e privada (assimétrica) auxilia a proteção contra o ataque de repetição durante a requisição do dispositivo móvel para o ponto de acesso.

A chave assimétrica garante que o dispositivo legítimo possa decifrar a mensagem de autenticação através da chave privada (chave secreta). Apesar disso, a captura de quadros acontece de acordo com as mensagens do dispositivo móvel e ponto de acesso. Para prevenir este ataque o mecanismo de proteção deve verificar os quadros. A Figura 3 mostra a fase de autenticação durante o handover. Um dispositivo móvel (*UE*) segue o protocolo de autenticação de entrega quando um ponto de acesso (*AP*) está em seu alcance de comunicação direta. O dispositivo móvel possui sua identidade e chaves criptografadas. A mensagem de autenticação $M = (pID|IDAP|ts)$ é enviada para o ponto de acesso, onde pID representa a pseudo-identidade do UE. O dispositivo móvel calcula a assinatura $AS = H2(M) * sH1(pID)$, onde um *timestamp* é adicionado para auxiliar a prevenção de ataques de repetição e a mensagem indica uma operação de concatenação. Desta forma, todas as entidades da rede preservam a sincronização de tempo de mensagem através de um mecanismo de sincronização de tempo. Em seguida, o UE envia mensagens de solicitação de acesso $\{Mi, A\}$ ao *AP*. Deste modo, o UE calcula a chave compartilhada simétrica com $AP : Ki - 2 = e(sH1(ipID), H1(IDAP))$.

Após a recepção de $\{M, A\}$, o AP efetiva os procedimentos de verificação através do mecanismo de proteção. O AP também efetua suas tarefas de resposta de autenticação. Os tempos são verificados para auxiliar na prevenção do ataque de repetição. O tempo de envio incluído no pID auxilia a verificação do tempo de expiração da mensagem do serviço de autenticação. Através da atribuição dos parâmetros re-

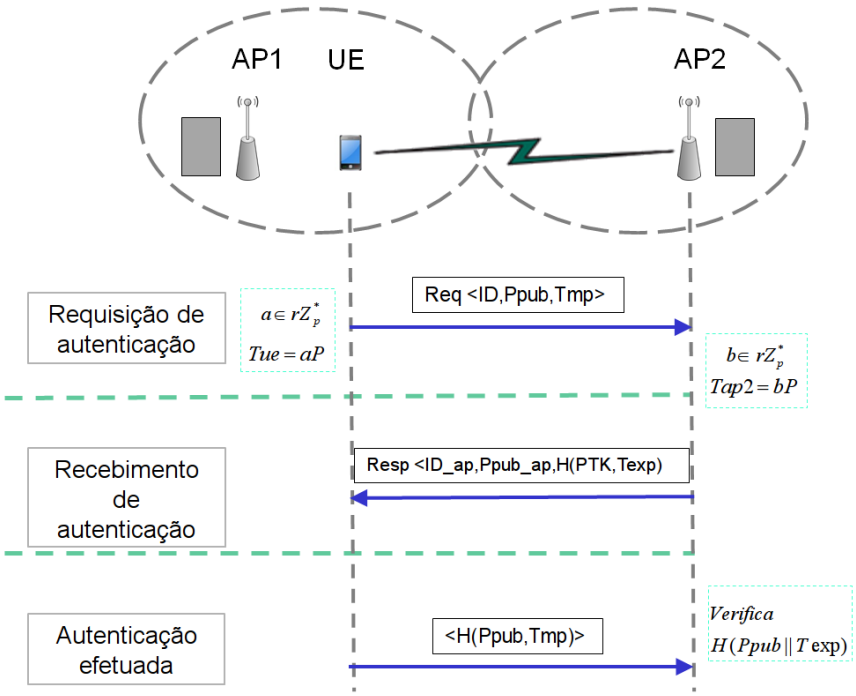

Figura 3. Autenticação

alizada pelo gerenciador central, o AP analisa se a assinatura A possui validade se $e(Ai, P) = e(H2(M) * H1(pID), pub)$. Então, $e(A, P) = e(H2(M) * sH1(pID), P)$ = $e(H2(M) * H1(pID), sP)$ = $e(H2(M) * H1(pID), pub)$.

O *AP* calcula ainda $K2 - i = e(H1(pID), sH1(IDAP))$. Os valores são analisados sendo $K2 - i = e(sH1(pID), H1(IDAP))$ = $e(H1(pID), H1(IDAP))$ $s = e(H1(pID), sH1(IDAP)) = K2 - i$. O AP gera um código de autenticação $Aut = H2(K - 2|pID|IDAP)$. Portanto, o AP envia as informações $\{pID, IDAP\}$ e *Aut* para o dispositivo móvel. Ao receber a mensagem $\{pID, IDAP, Aut\}$, dispositivo móvel gera um código de verificação $H2(Ki - 2|pID|IDAP)$ e compara com *Aut*. Se as informações $\{pID, IDAP\}$ e *Aut* corresponderem, o dispositivo móvel certifica-se que o AP é legítimo e estabeleceu uma chave *K* compartilhada 2-i; caso contrário, dispositivo móvel rejeita a conexão com o ponto de acesso.

3.3.3. Mecanismo de proteção

O mecanismo de proteção tem o objetivo de prevenir a personificação de identidade do ataque de repetição em redes que estejam no alcance do atacante no momento da captura de quadros. Este mecanismo atua no recebimento da mensagem de autenticação. A Figura 4 apresenta o mecanismo de proteção. Os módulos presentes no mecanismo de proteção são a verificação de tempo, verificação de quadros e atualização de conexão.

O módulo de verificação de tempo analisa o recebimento da mensagem *Trec*. Esta análise sucede da diferença do tempo de mensagem de autenticação enviada pelo usuário *Texp*, tal que *Texp* é embutida no quadro de autenticação, e o tempo de recebimento *Trec*. Desta forma, a diferença consiste de *Texp* - *Trec*. Este módulo fornece a garantia de que a

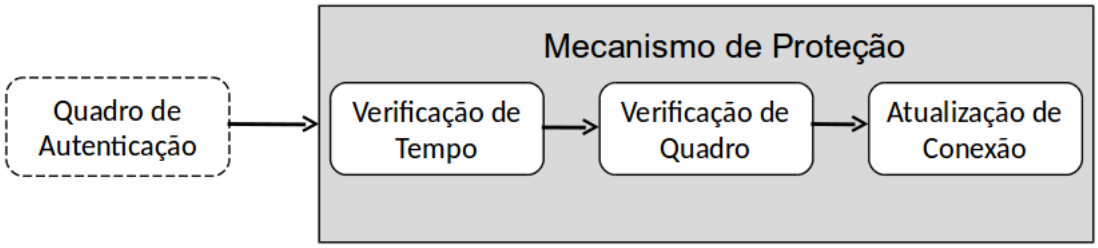

Figura 4. Mecanismo de Proteção

mensagem é única durante o periodo de tempo.

Cada quadro *qt* recebido pelo ponto de acesso detém sua identificação. A identificação é feita através da classificação de chegada de cada *qt*. Quando o quadro de autenticação *qt* chega no ponto de acesso, ele tem os campos analisados e classificado como *qt* = 1, e então outros quadros que possuam os mesmo campos de autenticação serão recusados. Esta estratégia invalida o ataque de repetição que visa a personificação de um dispositivo móvel. A estratégia também auxilia a caracterizar se este ataque esta sendo utilizado para efetuar negação de serviço. Para prevenir que o ataque seja efetuado em redes vizinhas, uma mensagem do ponto de acesso para os pontos de acesso vizinhos é enviada. Esta mensagem informa que o dispositivo móvel com uma identidade ID_i está conectado no ponto de acesso AP_i. Isso evita que o atacante propague a personificação em outras redes do ambiente sem fio.

O envio das mensagens ocorre entre as redes através da verificação do conjunto de redes vizinhas. As redes mais próximas serão informadas sobre a identidade e conexões de um dispositivo móvel. Um conjunto de vizinho *V* onde $V = \{ap_1, ap_2, ap_3, ..., ap_i\}$ tal que $ap_i \in V$. Para que a redes estejam completamente informadas sobre a conexão do usuário, o ponto de acesso envia a mensagem para o centro da rede de maior alcance, sendo a quantidade de mensagens *M* enviadas do AP para atualização de conexão representada por *M* onde $M = V + 1$. Este módulo informa os pontos de acesso vizinhos que o dispositivo móvel que possui uma identidade especifica esta conectado na rede.

4. Avaliação de Segurança e Desempenho

Esta seção apresenta a avaliação do esquema de controle de autenticação proposto para prevenir o ataque de repetição na autenticação do processo de *handover* em redes heterogêneas. Ele foi implementado no simulador NS-3, versão 3.24.1. O controle de autenticação foi avaliado levando em conta aspectos de segurança e desempenho da rede. Além disso, o esquema foi comparado com outra abordagem de autenticação chamada de UHA. A avaliação considerou um cenário composto por redes de diferentes tecnologias, dispositivos móveis e dispositivos maliciosos que executam o ataque de repetição.

O cenário utilizado na avaliação representa um ambiente de centro urbano com redes sobrepostas que possuem longo e curto alcance de sinal sem fio. Neste cenário representado pela Figura 5, os nós se movem no ambiente e utilizam o processo de transição de conexão nas redes sem fio. Logo, o serviço de autenticação prestará suporte ao processo de *handover* sempre quando for necessário a transição para outra rede. Os nós atacantes posicionam-se em partes do cenário onde existe grande sobreposição de redes. Desta forma, estes nós efetivam uma grande captura de quadros dispositivos móveis do

usuários legítimos presentes no cenário durante a autenticação na transição.

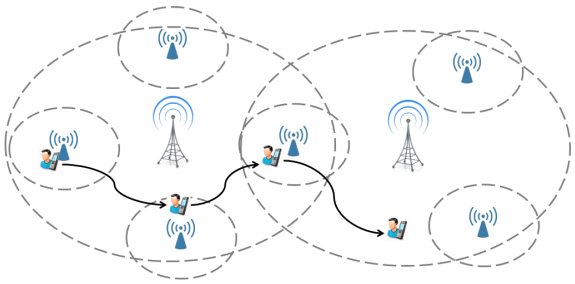

Figura 5. Cenário de Avaliação

Parâmetros	Valores
Quantidade de nós	20,40 e 60
Modelo de mobilidade	Random Waypoint
Velocidade dos nós	0,2m/s a 2m/s
Tempo de Simulação	600 s
Tecnologia	WiFi e LTE
Nós atacantes	10%

Tabela 1. Parâmet. de Simulação

A Tabela 1 dos parâmetros de simulação resume os valores usados na configuração das redes heterogêneas. O parâmetro da quantidade de nós na avaliação variou entre 20, 40 e 60. Os nós que compreendem os dispositivos móveis comum possuem mobilidade. Esta mobilidade é aleatória no cenário de avaliação com velocidades entre 2m/s e 5m/s. Os nós atacantes são fixos. A posição destes nós é aleatória em relação as localizações do cenário onde existem sobreposições de redes. A comunicação dos nós legítimos considera as tecnologias com padrões 802.11 (WIFI) e Long Term Evolution (LTE). A simulação foi repetida 30 vezes e cada simulação teve a duração de 600 segundos. A quantidade de atacantes representa 10% da quantidade de nós da avaliação.

As métricas para avaliar o controle de autenticação compreendem os aspectos de segurança e desempenho da rede. Os aspectos de segurança que relacionam o tipo do ataque consistem da taxa de detecção, taxa de falso positivo e taxa de falso negativo. A taxa de falso negativo não é levada para o contexto de avaliação pois não existem ocorrências para averiguar a métrica. As métricas de segurança usadas são a ***Taxa de ataques de repetição prevenidos*** (T_{prev}) e a ***Taxa de falso positivos*** (T_{fa}). A métrica T_{prev} representa os quadros repetidos descartados pelos esquemas que corresponde a razão entre o somatório de ataques prevenidos, *prev*, e a quantidade de ataques de repetição, *rep*, (Eq. 1). A métrica T_{fa} corresponde a quantidade de vezes que os esquemas identificaram um ataque quando não existia e é representado pelo somatório de prevenções, *prev*, pelo total de requisições de autenticação validas *req*, (Eq. 2).

$$T_{prev} = \frac{\sum prev}{rep} \quad (1)$$

$$T_{fa} = \frac{\sum prev}{req} \quad (2)$$

$$T_x = \frac{\sum T_{UE-AP}}{Q_{aut}} \quad (3)$$

$$T_y = \frac{\sum T_{AP-AP}}{msg} \quad (4)$$

$$T_z = \frac{\sum T_{AP-A}}{req} \quad (5)$$

$$C_{ini} = \frac{\sum T_{ini}}{Q_{ini}} \quad (6)$$

$$C_{aut} = \frac{\sum T_{aut}}{Q_{aut}} \quad (7)$$

As métricas de desempenho são ***Tempo médio de transmissão entre dispositivo móvel e ponto de acesso*** (T_x), ***Tempo médio de transmissão entre pontos de acesso*** (T_y), ***Tempo médio de transmissão entre ponto de acesso e autenticador*** (T_z), ***Custo computacional da inicialização*** (C_{ini}) e ***Custo computacional da autenticação*** (C_{aut}).

A métrica T_x consiste do somatório de tempo da transmissão entre o dispositivo móvel UE e o ponto de acesso AP, T_{UE-AP} e a quantidade de autenticações efetuadas Q_{aut}, (Eq. 3). A métrica T_y compreende o somatório de tempo da transmissão os pontos de acesso, T_{AP-AP} e a quantidade de mensagens enviadas msg, (Eq. 4). A métrica T_z compreende o somatório de tempo da transmissão entre o ponto de acesso, AP, e o autenticador A, T_{AP-A} em relação à quantidade de autenticações requisitadas entre eles req,(Eq. 5).

Já a métrica C_{ini} abrange a razão do tempo de todas as inicializações, T_{ini}, pela quantidade de inicializações efetuadas, Q_{ini}, (Eq. 6). A métrica C_{aut} representa o somatório do tempo de autenticação, T_{aut}, pela quantidade de autenticações, C_{aut}, (Eq. 7). Estas métricas de desempenho consistem do tempo em milissegundos gasto para concluir as tarefas tanto da transmissão como também o tempo para executar cada fase do esquema de autenticação.

4.1. Resultados

O Gráfico 6 mostra a taxa dos ataques de repetição prevenidos durante a simulação de 600 segundos. O esquema concorrente demonstra ser mais vulnerável por não possuir uma prevenção completa contra o ataque de repetição. Isto acontece em virtude da prevenção ser executada somente no mesmo ponto de acesso em que o nó legítimo está transitando. O controle de autenticação proposto (CAH) previne o ataque de repetição de forma mais abrangente, ou seja, levando em conta todas as possibilidades de ataque.

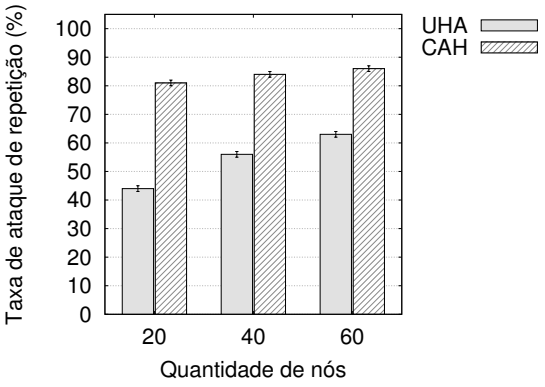

Figura 6. Taxa de prevenção

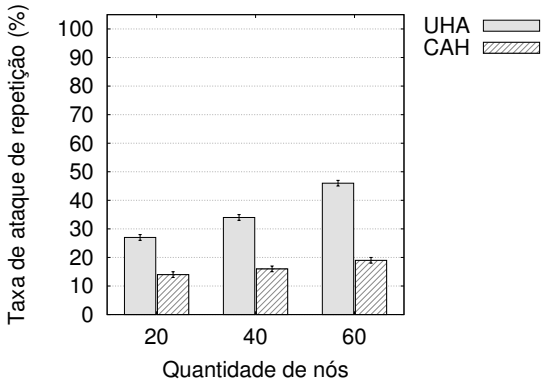

Figura 7. Taxa de falsos positivos

O Gráfico 7 mostra a comparação da taxa de falsos positivos. O esquema UHA apesar de não levar em conta todos os casos possíveis deste ataque, possui uma taxa de

falso positivo maior que o CAH. Isso ocorre em virtude dos outros ataques serem prevenidos de forma mais eficaz pelo mecanismo de proteção do CAH que leva em consideração o tempo e quantidade de mensagem. O componente de informação deste mecanismo consegue eliminar os ataques nas redes vizinhas de forma eficaz.

O Gráfico 8 apresenta a taxa total de ataques contra os tipos de tecnologias de redes. Esta diferença ocorre devido à característica de comunicação de cada tipo de rede ser diferente e pela variação de mobilidade dos dispositivos móveis. Isto proporciona aos dispositivos maliciosos uma maior capacidade para efetuar ataques. O gráfico 9 expõe a taxa total de ataques prevenidos em cada tipo de tecnologia.

A diferença de resultados compreende as características propostas por cada esquema de autenticação. O esquema UHA possui um tratamento de mensagens de autenticação efetivo em redes WiFi enquanto o esquem CAH impede ataques nas duas tecnologias. Isto ocorre pelo motivo da ausência de um tratamento do UHA em mensagens de ambas as tecnologias permitindo que o atacante obtenha o acesso pela identidade na rede de maior alcance e com isso usufruir dos serviços.

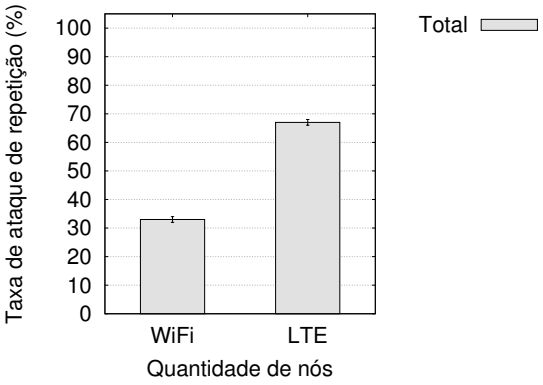

Figura 8. Taxa de ataques por tecnologia de rede

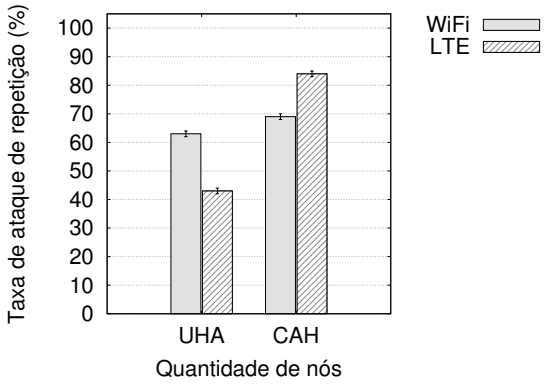

Figura 9. Taxa de prevenção por tecnologia de rede

Para avaliar o desempenho do esquema CAH com o UHA foi levado em conta a comparação da transmissão das mensagens e o custo computacional. O custo de transmissão da mensagem de autenticação consiste da comunicação entre o UE e o AP, o custo entre APs e entre o AP e o servidor de autenticação (AU), respectivamente. Desta forma, a Tabela 2 mostra as despesas gerais de transmissão dos sistemas de comunicação, e representa o desempenho das comunicações entre as entidades da rede heterogênea. As comunicações consistem do dispositivo móvel e ponto de acesso (UE-AP), do ponto de acesso com ponto de acesso (AP-AP), e do ponto de acesso e autenticador central (AP-A). A diferença de tempo está na relação da comunicação entre o dispositivo móvel e o ponto de acesso devido ao uso do pareamento que representa um método de processamento rápido para cifrar a informação.

Esquema	UE-AP	AP-AP	AP - A
UHA	4 ms	0	2 ms
CAH	2 ms	0	2 ms

Tabela 2. Comparação de transmissão

Esquema	Tempo de Inicialização	Tempo de *handover*
UHA	3 ms	4.5 ms
CAH	3 ms	2 ms

Tabela 3. Comparação de custo computacional

A Tabela 3 mostra uma comparação do custo computacional do esquema de autenticação UHA com o CAH. O pareamento obteve uma autenticação mais rápida em relação a troca de mensagens. O controle de autenticação CAH mostrou-se mais seguro e com melhor desempenho de comunicação em relação ao concorrente UHA. Isto se deve pelo motivo do pareamento ser realizado de forma unificada entre as redes possibilitando ao serviço de autenticação uma execução mais rápida.

5. Conclusão

Este trabalho apresentou o controle de autenticação (CAH) que possibilita uma melhor gerência dos dispositivos móveis nas redes heterogêneas e uma prevenção do ataque de repetição mais robusta no serviço de handover. Este controle consiste de um esquema de autenticação composto por duas fases e um mecanismo de proteção. As fases compreendem a autenticação inicial dos dispositivos móveis com a rede de maior alcance de transmissão sem fio e a autenticação no serviço de *handover* nas redes heterogêneas. O mecanismo realiza a proteção das informações de autenticação durante o *handover* e informa as redes vizinhas sobre os dispositivos autenticados. Para isso, o mecanismo executa a análise do tempo e da quantidade dos quadros de transmissão da autenticação recebidos na rede, e informa às redes vizinhas sobre a autenticação do dispositivo móvel com o propósito de evitar ataques e melhorar o desempenho da autenticação no serviço de *handover*. O controle de autenticação foi avaliado através do simulador NS-3 e a biblioteca crypto++. As simulações demonstraram que o controle de autenticação proposto através do uso de um esquema unificado de autenticação permite a prevenção de ataques de captura e melhora o desempenho do *handover*. Trabalhos futuros envolvem a análise da autenticação em relação à outros tipos de ataques que afetam a segurança das redes heterogêneas.

Referências

Cao, J., Ma, M., and Li, H. (2012). Unified handover authentication between heterogeneous access systems in lte networks. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 5308–5313. IEEE.

Cao, J., Ma, M., Li, H., Zhang, Y., and Luo, Z. (2014). A survey on security aspects for lte and lte-a networks. *Communications Surveys & Tutorials, IEEE*, 16(1):283–302.

Cheng, S.-M., Ho, C.-H., Chen, S., and Chang, S.-H. (2014). Distributed anonymous authentication in heterogeneous networks. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International*, pages 505–510.

Cremers, C. (2008). On the protocol composition logic pcl. In *Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 66–76. ACM.

Damnjanovic, A., Montojo, J., Wei, Y., Ji, T., Luo, T., Vajapeyam, M., Yoo, T., Song, O., and Malladi, D. (2011). A survey on 3gpp heterogeneous networks. *Wireless Communications, IEEE*, 18(3):10–21.

Feng, T. and Jiao, J. (2012). WAPI secure access authentication scheme for heterogeneous networks based on identity-based cryptograph. In *Computing Technology and Information Management (ICCM), 2012 8th International Conference on*, volume 1, pages 130–135. IEEE.

Fu, A., Zhang, G., Zhang, Y., and Zhu, Z. (2013). Ghap: An efficient group-based handover authentication mechanism for ieee 802.16 m networks. *Wireless personal communications*, 70(4):1793–1810.

He, D., Chan, S., and Guizani, M. (2015). Handover authentication for mobile networks: security and efficiency aspects. *Network, IEEE*, 29(3):96–103.

He, D., Chen, C., Chan, S., and Bu, J. (2012). Secure and efficient handover authentication based on bilinear pairing functions. *Wireless Communications, IEEE Transactions on*, 11(1):48–53.

Heath, R., Kountouris, M., and Bai, T. (2013). Modeling heterogeneous network interference using poisson point processes. *Signal Processing, IEEE Transactions on*, 61(16):4114–4126.

Hu, Y.-C., Perrig, A., and Johnson, D. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1976–1986 vol.3.

Kent, A. D., Liebrock, L. M., and Neil, J. C. (2015). Authentication graphs: Analyzing user behavior within an enterprise network. *Computers & Security*, 48(0):150 – 166.

Li, X., Zhang, Y., Liu, X., Cao, J., and Zhao, Q. (2012). A lightweight roaming authentication protocol for anonymous wireless communication. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 1029–1034. IEEE.

Ranjan, S., Akhtar, N., Mehta, M., and Karandikar, A. (2014). User-based integrated offloading approach for 3GPP LTE-WLAN network. In *Communications (NCC), 2014 Twentieth National Conference on*, pages 1–6.

Sandhu, R. and Samarati, P. (1994). Access control: principle and practice. *Communications Magazine, IEEE*, 32(9):40–48.

Xenakis, D., Passas, N., Merakos, L., and Verikoukis, C. (2014). Mobility management for femtocells in lte-advanced: Key aspects and survey of handover decision algorithms. *Communications Surveys Tutorials, IEEE*, 16(1):64–91.

Yu, Q., Jiang, W., and Xiao, Z. (2013). 3g and wlan heterogeneous network handover based on the location information. In *Communications, Circuits and Systems (ICCCAS), 2013 International Conference on*, volume 2, pages 50–54. IEEE.