UNIVERSIDADE FEDERAL DO AMAZONAS
PRO REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

ESTUDO DE SEGURANÇA DE ACESSO EM REDES OPORTUNISTAS

BOLSISTA: João Victor Lima Lopes, CNPQ

MANAUS
2014

UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RELATÓRIO FINAL
(PIB-E/0187/2013)
ESTUDO DE SEGURANÇA DE ACESSO EM REDES OPORTUNISTAS

BOLSISTA: João Victor Lima Lopes, CNPQ
ORIENTADOR: Prof° Dr° Edson Nascimento Silva Junior

MANAUS
2014

Resumo

Um novo tipo de conexão vem sendo desenvolvido para suprir necessidades globais em relação a troca de mensagens e dados em geral, as Redes Oportunistas[2][3]. Com o objetivo de contribuir para essa nova tecnologia, começamos um projeto para pesquisa de métodos de segurança abordados em redes e conexões já existentes para que esses pudessem ser adaptados e adequados para que fossem úteis também nas Redes Oportunistas.

Ao longo do desenvolvimento dessa pesquisa vimos a oportunidade de desenvolver uma nova forma de proteção de dados e não apenas adaptar uma já existente. Com esse pensamento, direcionamos os esforços para fortalecemos as bases e fundamentos teóricos que pudessem apoiar nossas ideias.

Assim, partimos para o projeto de algoritmos baseados em tecnologia genética. Ainda nos encontramos em uma fase não conclusiva, trabalhando dentro da potencialidade das ideias a serem inseridas no algoritmo.

Sumário

1. Introdução..... 5

2. Revisão Bibliográfica..... 6

3. Métodos Utilizados..... 8

4.Resultados e Discussões.…..... 9

5. Fontes e Referências Bibliográficas..... 11

6. Cronograma..... 12

1. Introdução

As Redes Oportunistas surgiram com o objetivo de mitigar os problemas comuns à cenários de comunicação de topologia dinâmica [2]. Os nós (receptores e transmissores) se encontram em constante movimento e o crescimento de conteúdos gerados por usuários de *smartphones* e compartilhamentos desses conteúdos através de redes sociais como Facebook, Youtube e Instagram, lançou as operadoras de telefonia celular em uma corrida para atender a crescente necessidade da capacidade dos seus serviços de transmissão de dados (downstreaming e upstreaming) [1], visando encontrar uma alternativa para esses problemas atuais, e que tendem a ficar cada vez pior, está sendo desenvolvida uma pesquisa para tratar de uma nova forma de comunicação entre dispositivos, as Redes Oportunistas [3]. Essas redes têm como objetivo fazer um trafego de arquivos sem a necessidade de recorrer a conexões de internet (3G,4G ou WI-FI), fazendo assim o usuário ter um gasto menor de banda, evitar congestionamento da rede e evitar também gastos financeiros. Redes Oportunistas tem como principio básico, fazer com que usuários consigam enviar e receber arquivos diretamente de um dispositivo para o outro, além disso, fazer com que esses mesmos usuários consigam, através de um mapeamento desenvolvido, enviar arquivos de um usuário para o outro, passando antes por qualquer que seja outro dispositivo (Transportador), fazendo com que pessoas consigam levar informações de umas para outras de graça e usando conexões de internet somente em últimos casos [1].

Esse tipo de conexão, assim como qualquer outra, precisa de segurança, nosso objetivo principal é desenvolver métodos seguros e eficientes de proteção para quando e se essa tecnologia vier à funcionar possa ser capaz de trabalhar sem que haja problemas de invasão ou perda de dados e espionagem, para que seus arquivos trafegados possam estar tão ou mais seguros do que dados trafegados em e-mail por exemplo.

A princípio, gostaríamos de pesquisar métodos já existentes em outros tipos de comunicação e adaptá-los para essa nova tecnologia, mas após várias pesquisas e levantamentos, observamos a oportunidade de desenvolver um novo método de proteção. Com esse propósito pesquisamos vários métodos existentes que pudessem dar base e fundamentos para nosso trabalho, conseguimos utilizar alguns métodos, como o PGP [4] que é de uso livre e foi fundamental para ser o alicerce do algoritmo pretendido.

Tomamos então uma linha principal de pesquisa e desenvolvimento, que é a pesquisa para desenvolvimento de uma nova forma de Criptografia, que será usada para proteção de textos e pacotes de dados que trafegarão na Rede Oportunista, dependendo da sua qualidade e eficiência, quem sabe possa ser um algoritmo também aproveitado para outras tecnologias.

2. Revisão Bibliográfica

De acordo com o Estudo Preliminar Sobre Disseminação de Conteúdo em Redes Oportunistas feito em 2012 [2], o conteúdo gerado por celulares e smartphones vinham crescendo rapidamente. Segundo dados, no ano de 2014 estaríamos utilizando em média 7GB de tráfego por mês, o que representava 5,4 vezes mais do que era medido em 2012. Os principais responsáveis por esse grande aumento sem dúvida são as redes sociais. Os conteúdos gerados pelos usuários e compartilhados por essas redes, como Facebook, Whatsapp, Instagran e Youtube, é muito grande, e as operadoras telefônicas principalmente, se viram obrigadas a correr contra o tempo para poder dar conta de tanta demanda. A partir dessa necessidade, várias pesquisas e tecnologias estão sendo desenvolvidas com o objetivo de diminuir o máximo o tráfego de dados entre usuários e as operadoras, os esforços estão concentrados em métodos de tráfegos entre os próprios usuários, chamados tráfegos horizontais, esses seriam capazes de reduzir bastante a quantidade de tráfego entre esses dispositivos e operadora, o que ajudaria a dar conta da demanda, melhorar outros serviços das operadoras como as chamadas convencionais e outros, além de atender novos clientes que vierem a necessitar do serviço (Rodrigues, A, 2012)[2]. Esse estudo foi muito bem elaborado, demonstra de forma clara o que significa Redes Oportunistas e suas necessidades, foi fundamental para nos guiar em nossas pesquisas, baseados nesse estudo também, vimos a necessidade de contribuir para algo que sem dúvida será uma necessidade em breve, esse foi o primeiro passo para que iniciássemos nossa linha de pesquisa, nossa abordagem e objetivo.

Para iniciar nossas pesquisas, precisávamos de noções básicas de segurança, para isso foram feitas várias pesquisas com base nas ferramentas de segurança utilizada em e-mails e outros tipos de trocas de mensagens e dados, constatamos que o princípio básico de segurança dessas tecnologias é a criptografia, ela é a parte fundamental para que se tenha proteção nos dados trocados entre dois ou mais usuários, além dela há também outros métodos que garantem a origem da mensagem e sua autenticidade [Stallings. W, 2008][4].

Através dessas analises, direcionamos nossas pesquisas para identificar as ferramentas mais modernas e mais utilizadas. Encontramos então muitas referências que apontam para um método de criptografia que é amplamente utilizado e muito recomendado, o AES, que é um método que está hoje em pelo menos 70% das novas aplicações que possuem necessidade de proteção. Depois de passar cerca de 5 anos em um processo de padronização, foi anunciado em 2001 como algoritmo oficial do governo dos EUA, isso o tornou bastante popular, tendo em vista que antes dele, havia o DES, que é também um algoritmo de criptografia que estava defasado, pois o tamanho da chave o que o mesmo

utiliza é considerada pequena para o poder computacional existente, isso o tornou bastante vulnerável, apesar de ainda ter algumas aplicações que utilizam em uma versão mais complexa, 3DES, que nada mais é que o mesmo algoritmo executado 3 vezes[5].

Isso nos deu uma direção mais precisa para nossa pesquisa, pois com base nessas referencias decidimos seguir o caminho do desenvolvimento de um novo modelo criptográfico, só que diferente do algoritmo AES, que usa um modelo de Chave Simétrica[6].

O modelo de criptografia com chave simétrica é um algoritmo que se utiliza de uma única chave, que tanto o destinatário quanto o remetente precisa ter conhecimento, esta chave é aplicada no momento que o algoritmo está sendo executado, ou seja, no momento que está ocorrendo a encriptação da mensagem[6]. Essa chave é muito importante para o bom funcionamento da proteção, se ela for fraca, descoberta ou pequena a ponto de ser atacada por *brute-force* [7], o algoritmo por mais complexo que seja é totalmente inútil, pois essa chave é a parte fundamental do algoritmo.

Seguindo essas definições, imaginamos que teríamos mais proteção se utilizássemos um algoritmo tão bom quanto o AES, porém com chave *assimétrica*, que é o contrário da chave simétrica, ou seja, não há apenas uma chave, mas sim, duas (um par) para cada usuário, uma chave chamada privada, que é de conhecimento exclusivamente do remetente e uma pública, que é amplamente distribuída para todos que necessitam dela. Assim como o remetente tem seu par de chaves, o destinatário também tem, só que claro, são totalmente diferentes [6].

Com esse levantamento então é que se baseia nossa pesquisa, tentar dar uma qualidade maior para um algoritmo, fazendo com ele trabalhe com chaves assimétricas. Não visamos incrementar o algoritmo AES já existente, mas sim procurar desenvolver um algoritmo que além de trabalhar com chave assimétrica, ele possa ser mais eficiente em tempo de execução e que tenha uma característica de mutação, característica essa que ainda é apenas uma ideia, não foi pesquisada ainda a sua possibilidade, mas tentaremos dar mais essa forma de proteção para um algoritmo sem que esse perca a eficiência, pois há várias aplicações de algoritmos mutáveis, conhecidos com *Algoritmos Genéticos* ou *Algoritmos Evolutivos,* que são utilizados em sua maioria para otimização de soluções computacionais, mais direcionadas à buscas, esse algoritmos tendem a se ajustar conforme a necessidade do problema, apesar dele ser considerado lento, é muito utilizado[7].

Uma ferramenta que será importante também em nosso desenvolvimento é a PGP, que é fundamental para se trabalhar com chaves assimétricas[4].

3. Métodos Utilizados

Nossa metodologia foi totalmente centrada em pesquisa, pois o que estávamos propostos a fazer no começo do projeto, era a adaptação de uma tecnologia de segurança já existente, de forma que essa viesse a ser útil para as Redes Oportunistas.

Como citado anteriormente, o desenvolvimento do trabalho nos oportunizou a buscar um caminho diferente do previsto, tomando por base conhecimento levantado no início do projeto. Assim, observamos uma oportunidade de desenvolver uma nova tecnologia em vez de apenas adaptar uma já existente.

Com esse objetivo, novamente, utilizamos de pesquisas para delimitar um caminho para seguir, encontrar métodos existentes para que não fizéssemos igual e também outros que viessem a ser útil para nosso algoritmo.

Após os primeiros levantamentos, partimos para a fase de desenvolver o algoritmo que seria aplicado para encriptação de mensagens. Por vezes, foram necessárias revisões das sequências de ações, e observarmos e avaliarmos comportamento do algoritmo, através de implementações parciais de código em Linguagem C, para fazermos testes e simulações.

Temos como meta implementar e realizar testes de eficiência e corretude para comparar nosso algoritmo com o algoritmo AES, que é o mais utilizado e recomendado.

4.Resultados e Discussões

Nossos resultados não encontram-se em fase conclusiva, visto que precisamos ainda fazer ponderações no desenho dos algoritmos para então colocá-los em desenvolvimento, e só então realizar os testes de eficiência, corretude e comparativos.

Somente ao final de todo o processo, podermos dar maior precisão ao que estamos realizando. Infelizmente, a pesquisa apresentou maior volume de trabalho do que previsto, visto se tratar agora do desenvolvimento de um novo algoritmo de segurança de dados, com mecanismos de criptografia diferente do que convencionalmente se utiliza.

Conforme o esboço do algoritmo abaixo, definimos um caminho, e, conforme o andar das atividades, sempre nos deparamos com necessidades de mudança, fato que ocorreu sobremaneira. Levando em consideração a figura abaixo, fica claro que é uma definição que está em pleno desenvolvimento e pouco conclusiva, portanto; isso se da pelo fato do formato que estamos trabalhando, seguindo os conceitos do algoritmo PGP[4], pudemos estruturar de forma bastante simples o que pretendemos seguir, essa figura é o caminho básico para que possamos seguir com a pesquisa, porque o que a parte principal é o que acontece nas operações de manipulação de chaves e codificação e descodificação da mensagem, essas são, sem dúvida, os objetos principais da nossa pesquisa.

As operações que estamos definindo vão definir a qualidade da nossa proposta de algoritmo, dando a eficiência e robustez do nosso trabalho. As operações de manipulação de chave e de encriptação da mensagem ainda estão aguardando definições mais precisa, em vista de termos trabalhado em diferentes ideias, vários métodos novos que serão importantes para a nosso métodos. Assim, trabalhamos com várias ideias que podiam ser usadas, e ainda trabalhamos no momento com ideias novas que estão sendo adaptadas e ajustadas para que possamos ter uma boa eficiência.

Não citaremos com detalhes esses métodos pois estamos avaliando a sua utilidade para o trabalho, decidimos apenas apresentar o esboço do algoritmo pois esse sim, terá sua maior parte aproveitado, suas características de chaves públicas e privadas também, além das ideias de transição, provavelmente no futuro, esse será a base para realizar as operações de encriptação.

Durante o processo de desenvolvimento, discutimos muito sobre o que seria adequado, na verdade foram levantadas vária hipóteses, inclusive de se trabalhar com algoritmo quântico, mas foi inviabilizada, pelo menos em sua totalidade, pois vários fatores que são aplicados a criptografia quântica, como a transmissão de dados através de lasers ou o fato de por enquanto só se poder fazer essa comunicação apenas entre dois computadores, não podem ser aplicados em dispositivos comuns, mas em geral, a

criptografia quântica com certeza é promissora, pois tem uma característica que é muito importante: de acordo com os princípios da física quântica, o observador de um experimento tem influência direta no resultado, as partículas se comportam de forma diferente quando são diretamente medidas ou não, desta forma, se houver algum tipo de escuta, a interferência será percebida imediatamente e a transmissão da informação será interrompida.

Essa característica de observar se a mensagem foi lida ou interceptada antes de chegar ao destinatário é muito útil, pois seria fundamental para analisar se alguma instituição ou pessoa está sendo monitorada ou espionada. Gostaríamos de utilizar um método parecido em nosso algoritmo, mas veremos a sua possibilidade mais para frente.

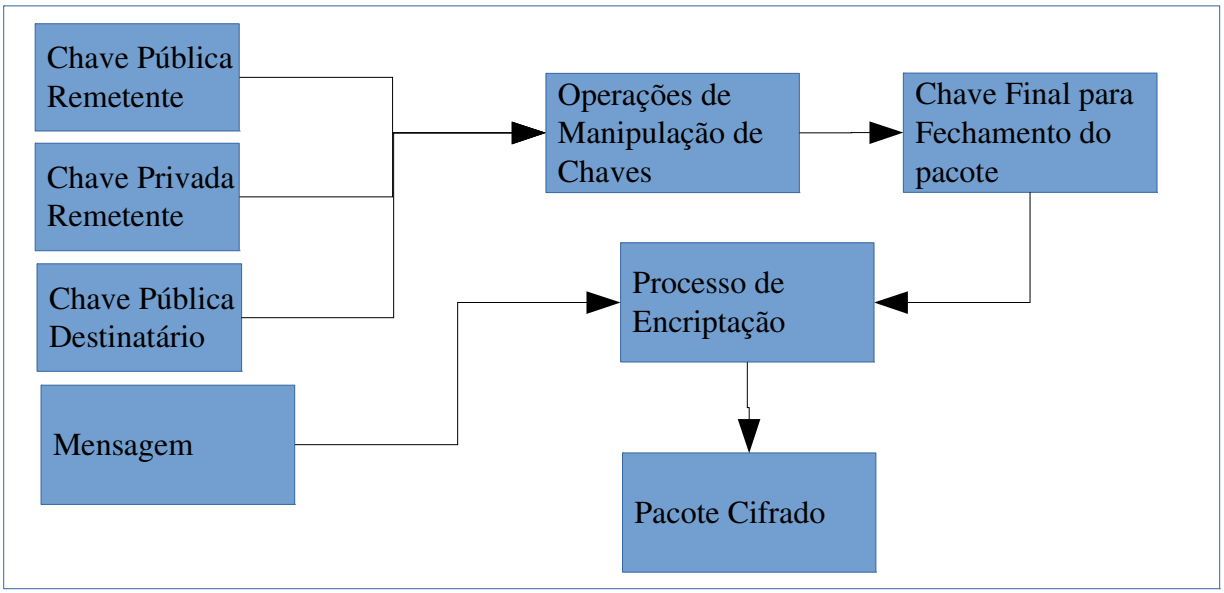

Figura 1: Processo de Cifragem do pacote.

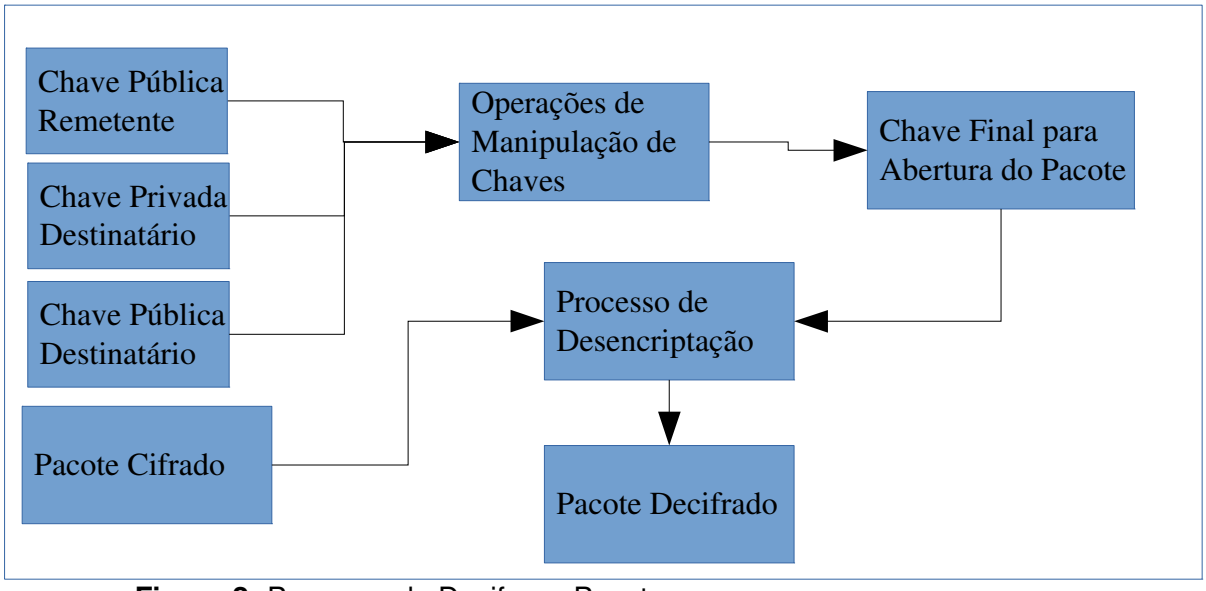

Figura 2: Processo de Decifrar o Pacote.

5. Fontes e Referências Bibliográficas

[1] K. Lee, I. Rhee, J. Lee, Y. Yi, and S. Chong, ***Mobile data offloading: How much can wifi deliver?*** in *SIGCOMM'10*. ACM, September 2010.

[2] RODRIGUES, A, ***Estudo preliminar sobre disseminação de conteúdo em redes oportunistas***.

[3] ——, "**Modelling data dissemination in oppor tunistic networks,**" in CHANTS'08. ACM, September 2008.

[4] *Stallings, W,* ***Criptography and Networking Security.*** *4.ed. São Paulo: Pearson Prentice Hall, 2008. 476 p.*

[5] Trevissan, D. F; Sacchi, R.P da S; Sanabria, L. **Estudo do Padrão Avançado de Criptografia AES – Advanced Encryption Standard. RITA, Volume 20, Número 1.** Disponível em: http://seer.ufrgs.br/rita/article/download/rita_v20_n1_p13/23763,. Acesso em: Jan. 2014.

[6] *Oliveira, R.O,* ***Criptografia simétrica e assimétrica: os principais algoritmos de cifragem.*** *Revista* Segurança Digital - 3ª ed. Nov. 2013. Disponível em: http://www.segurancadigital.info/pagina-inicial/451-seguranca-digital-3o-edicao-novembro- . Acesso em Jan 2014.

[7] Pacheco, M. A. C. **Algoritmos Genéticos: Princípios E Aplicações**. PUC, Rio de Janeiro. Disponível em: <http://www.ica.ele.puc-rio.br/downloads/38/ce-apostila-comp-evol.pdf> Acesso em: Dez. 2013.

6. Cronograma

Nº	Descrição	Ago 2013	Set	Out	Nov	Dez	Jan 2014	Fev	Mar	Abr	Mai	Jun	Jul
1	Fazer um levantamento das principais ferramentas que possam ser empregadas no projeto.	P C											
2	Estudar e conhecer as principais ferramentas levantadas, definindo uma a ser empregada ao longo do projeto.		P C	P C									
3	Conhecer os métodos já desenvolvidos e pesquisas já realizadas para aprimorar o conhecimento em relação a esse projeto.				P C								
4	Aprender a linguagem de desenvolvimento mais utilizada para os dispositivos que se pretende trabalhar (JAVA).					P C	P C	P C					
5	Verificar quais são as necessidades de segurança, o que se deseja proteger e como.								P C				
6	Utilizar de métodos pesquisados para organizar ideias relativas ao desenvolvimento do trabalho.									C			
7	Aplicar os métodos relacionados como úteis para serem aplicados no algoritmo base.										C		
8	Fazer testes com esses métodos pesquisados ou desenvolvidos, a fim de aprimorá-los e adequá-los.									P	P	P	
9	Fazer a integração dessa pesquisa com o projeto principal ao qual se pretende desenvolver em paralelo.												P

10	Elaboração do Resumo e Relatório Final (atividade obrigatória)												**P** **C**
11	- Preparação da Apresentação Final para o Congresso (atividade obrigatória)												**P** **C**

P: Previsto, **C**: Concluído.