

CRIPTOGRAFIA FORTE APLICADA EM REDES MANET

Marcelo Fernandes de Freitas, Marcos Antonio Cavenaghi, Cleber Morio Okida, Roberta Ulson Spolon, Aparecido Nilceu Marana. – Ciência da Computação – Bacharelado em Ciência da Computação – Departamento de Computação – Faculdade de Ciências – Campus de Bauru

O poder de um algoritmo criptográfico é medido pelo tempo de execução e pelos recursos que devem ser gastos para repor o texto original. O resultado da criptografia forte é texto cifrado, muito difícil de quebrar sem o uso da ferramenta adequada. Este trabalho fez uma avaliação de desempenho de algoritmos de encriptação quando utilizados em redes MANET (Mobile Ad Hoc Networks). Para isso, os tempos de execução do algoritmo AES (criptografia simétrica) foi avaliado, após ser integrado ao código fonte do NS (Network Simulator)[VINT 1996][OTCL 1997].

O algoritmo AES foi escolhido, pois é bastante utilizado e também recomendados nos documentos da biblioteca NIST (National Institute of Standards and Technology). Mobile Ad Hoc Networks (MANET) compõem-se de um conjunto de nós autônomos que se comunicam sobre links sem fio (wireless) com capacidade limitada, tanto de largura de banda quanto de potência de transmissão e processamento [NIST 2005][VINT 1996].

Estes estudos envolveram o desenvolvimento de aplicações móveis simples escolhidas de forma a possibilitar o entendimento dos mecanismos envolvidos nas simulações com o NS, tais como os protocolos de roteamento e a criação dinâmica de novos links entre os nós da rede. Tais estudos possibilitaram ao autor a familiarização com a ferramenta de simulação NS além de possibilitar o entendimento dos fatores envolvidos em criptografia forte em redes MANET [TOH 2002].

O tráfego escolhido para implementação do sistema foi o padrão IEEE 802.11, que define a camada física e de enlace da rede. A taxa do canal é de 11 Mbps [IEEE 2004]. O protocolo de roteamento usado é o *Ad Hoc On-Demand Distance Vector* (AODV), utilizado em redes *Ad Hoc*. O protocolo de transporte é o *User Datagram Protocol* (UDP), sendo o tráfego gerado pela fonte do tipo *Constant Bit Rate* (CBR) de 1 Mbps [VINT 1996]. A métrica escolhida para análise dos protocolos foi a taxa de entrega de pacotes. A taxa foi definida como a relação entre o número de pacotes originados pelas fontes CBR do nó de origem e o número de pacotes recebidos pela fonte CBR do nó de destino [IEEE 2004] [MONARCH 2003]. O Network Simulator [OTCL 1997] foi a ferramenta escolhida para estudar o comportamento dos vários fatores envolvidos em redes MANET, pois é uma ferramenta desenvolvida em C++ e Otcl [OTCL 1997] para simulação dos vários aspectos envolvidos nas Redes de Computadores. Com resultados precisos nas simulações (resultados obtidos com o NS são praticamente os mesmos aos obtidos em redes reais).

As avaliações foram baseadas em simulações de 5 terminais móveis que formavam uma rede *Ad Hoc*, disposta sobre uma área retangular de 1500m x 1500m, durante um tempo de 900 segundos, com a finalidade de avaliar o impacto na comunicação de apenas dois nós. A taxa de entrega de pacotes é uma métrica importante, porque descreve a taxa de perda dos pacotes, o que afeta a vazão máxima que a rede pode suportar. Essa métrica caracteriza a eficácia do protocolo da rede.[NIST 2005] Cabe ressaltar que os tempos necessários para estabelecimento das chaves também foram considerados, sobretudo em cenários em que não exista qualquer prévio contato entre os nós, pois neste ambiente exige-se inicialmente um volume intenso de mensagem para que cada nó obtenha suas chaves, aumentando assim o tempo de processamento de mensagens nos sistemas com segurança, em relação aos sistemas sem segurança.

A implementação de AES que usa 128 e 256 bits de dados com um clock de 50 MHz tem um processamento de 200 Mbits/s. Dessa forma, executa os 1024 bytes de dados em um tempo aproximado de 41 μ s. As taxas de transmissão obtidas foram computadas levando-se em consideração os valores típicos usados para cifrar e decifrar, que na expressão matemática da chave. Esses valores têm a largura de 12 bits e 30 bits para cifrar, e de 20 bits e 50 bits para decifrar. São valores considerados típicos para chaves de 128 e 256 bits de tamanho [NIST 2005].

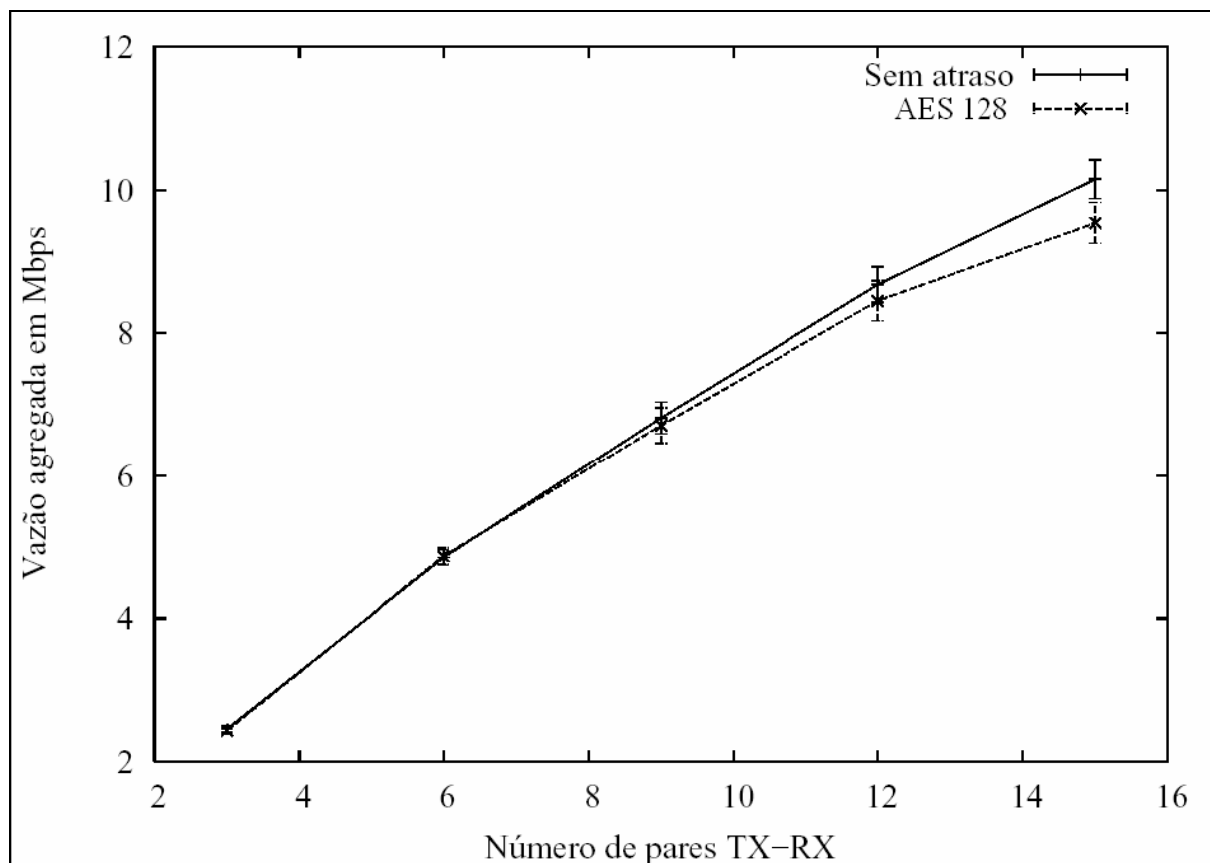


Figura 1 : Vazão da rede com o AES com chave de 128 bits

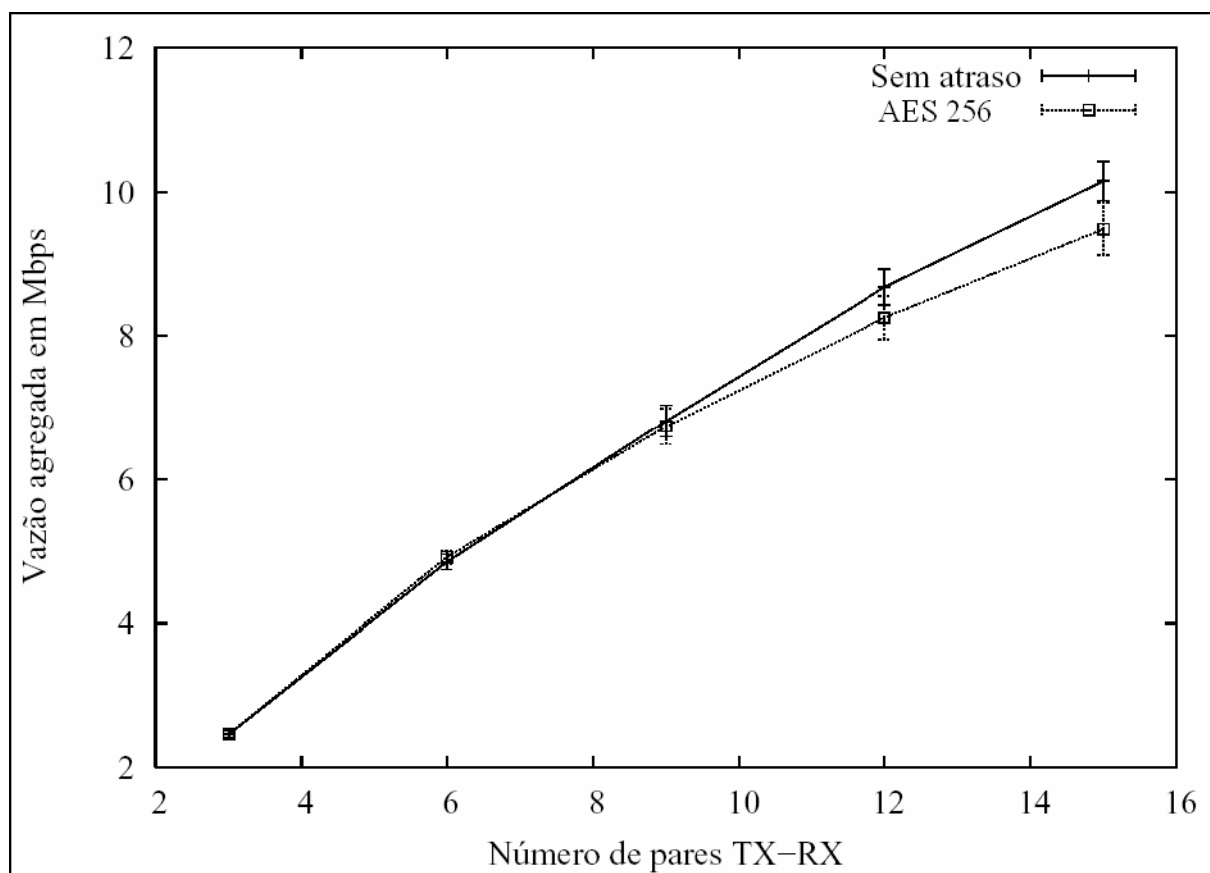


Figura 2 : Vazão da rede com AES com chave de 256 bits

Sem as chaves privadas não se pode decifrar as mensagens passadas entre os dois terminais e o desempenho global é tão rápido que para uma mensagem de 1024 bytes de dados, o processo dura aproximadamente 53 ms. Porém, se forem transmitidos 10 pacotes de dados de 1024 bytes, durará menos que 54 ms, pois a sessão que codifica a chave privada do AES é realizada apenas uma vez com o algoritmo.

A frequência de operação do AES foi de aproximadamente 15 MHz, para chaves de 256 bits, o que é muito aceitável para um circuito que calcula o módulo da exponencial de números longos.

O valor obtido para o consumo de energia no processamento de mensagens de 1024 bytes do circuito AES (384,5 mJ) pode ser considerado elevado em relação a outros circuitos que implementam outros algoritmos, tendo em vista o tempo de processamento da mensagem e a potência média consumida pelo circuito, de 1788 mW.

Contudo, para aplicações de curto processamento, como cifrar/decifrar chaves de algoritmos criptográficos simétricos, é satisfatório. Desse modo, pode-se comprovar que o Rijndael obteve um bom desempenho e atraso de pacotes pequeno, causando um menor impacto na execução da comunicação entre os nós da rede.

Com base nestes resultados das simulações será proposta a integração, aos protocolos de comunicações, dos mecanismos de segurança de criptografia assimétrica, como o RSA, para posterior comparação de desempenho [KÄRPIJOKI 2001]. Pois nenhum dos sistemas simétrico e assimétrico, separadamente, oferece total eficiência no processo de cifragem e decifragem, no que se refere a número de chaves, velocidade de processamento e distribuição de chaves.

Referências Bibliográficas

[IEEE 2004] IEEE standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. August 1999 <<http://pdos.csail.mit.edu/decouto/papers/802.11a.pdf>> Acesso em: mar 2004.

[KÄRPIJOKI 2001] KÄRPIJOKI, V., Security in ad hoc networks. In Seminar on Network Security, Sjukulla, Finland 2001.

[MANET 2002] Mobile Ad hoc Networks (MANET). Disponível em: <<http://www.ietf.org/html.charters/manet-charter.html>>, acesso em Set 2002.

[MENEZES 1997] MENEZES, Alfred J., P. C. V. O., VANSTONE, Scott A., Handbook of Applied Cryptography. CRC Press LLC, 1997.

[MONARCH 2003] MONARCH, Mobile Networking Architectures. Disponível em: <<http://www.monarch.cs.cmu.edu>>, acesso em abr 2003.

[NIST 2005] NIST. Guideline for Implementing Cryptography in *The Federal Government FIPS PUB 800-21 Release 1*, NIST, Setembro 2005

[OTCL 1997] OTcl; <<http://otcl-tclcl.sourceforge.net/otcl/>> Acessado em 31 de Janeiro de 2006

[VINT 1996] VINT Project — Virtual InterNetwork Testbed, <<http://www.isi.edu/nsnam/vint/>> Acessado em 31 de Janeiro de 2006.

[SCHNEIER 1996] SCHNEIER, Bruce, Applied Cryptography. Second Edition, John Wiley & Sons Inc., 1996.

[STINSON 2002] STINSON, Douglas R.; Cryptography : theory and practice — 2nd ed.; ISBN:1-58488-206-9, Chapman & Hall / CRC Press Company, 339 páginas, Janeiro 2002

[TOH 2002] TOH, C. K., Ad Hoc Mobile Wireless Network – Protocols and Systems. In 1st Edition, Prentice-Hall 2002.

Bolsa : não tem