Relacionando criptografia e consumo utilizando lógica *fuzzy*

Daniel Tadeu Martinez Castello Branco[1], Edson Nascimento Silva Júnior[1]

[1]Universidade Federal do Amazonas (UFAM)
Manaus – AM – Brasil

danielt@ufam.edu.br, edson@dcc.ufam.edu.br

Abstract. *Mobile devices characterize to have low battery resources. Meanwhile, cryptography can cause high processing levels, affecting the available energy. Using fuzzy logic, this works intends to find a balance between power consumption and security.*

Resumo. *Dispositivos móveis se caracterizam por possuir escassos recursos de bateria. Entretanto, a criptografia pode provocar altos níveis de processamento, afetando a energia disponível. Utilizando lógica fuzzy objetiva-se encontrar o equilíbrio entre consumo e segurança.*

1. Introdução

Quando se fala em redes de computadores, a mobilidade é uma característica que tem sido considerada nos últimos anos. Como resultado, maneiras tradicionais de comunicação apresentam-se inadequadas frente ao modelo de vida atual. Com isso, os dispositivos móveis são úteis para que o conceito de mobilidade seja fielmente usado.

O crescimento da utilização de redes sem fio e de dispositivos móveis, faz com que mais dados estejam suscetíveis. Diante disso, a garantia da integridade dos dados trafegados em uma rede de computadores é uma necessidade concreta (Jorstad, 1997). A criptografia tem por finalidade minimizar os riscos de que dados sejam violados, uma vez que passam por um processo de cifragem. Nesse contexto, se insere o processo de autenticação e criptografia de dados.

Considerada a validade do algoritmo em uma determinada situação e seu nível de segurança, um fator deve ser considerado: consumo de energia. Como o foco do trabalho é a sua aplicação em dispositivos móveis, a otimização do uso da bateria é uma variável que deve ser avaliada, uma vez que tais recursos são escassos.

Algoritmos de criptografia se caracterizam por serem computacionalmente custosos. Estes algoritmos são constituídos por seqüências complexas de instruções, repetições, permutação de valores, etc, o que acaba onerando o seu processamento, ou seja, são explorados recursos da CPU (processador), memória e de energia.

Assim, considerando a utilização de dispositivos móveis, o consumo de energia tem extrema relevância. Estabelecer o equilíbrio entre criptografia e consumo de energia é um grande desafio, já que há necessidade de manter os dados íntegros, sem existir consumo exacerbado de energia. Porém, a harmonia entre estas duas variáveis depende de conceitos não tão objetivos. Nesse cenário de subjetividade, a incorporação de técnicas mais abrangentes, como a lógica *fuzzy*, proporciona benefícios significativos, sendo útil na definição de valores menos intuitivos, reforçando a tomada de decisões mais precisas.

2. Trabalhos relacionados

(Jorstad, 1997) define uma métrica para qualificar um algoritmo. São propostas algumas variáveis a serem consideradas para concluir se um algoritmo pode ser considerado como bom ou ruim.

Para tentar minimizar o consumo de energia, estudos foram desenvolvidos, utilizando diversas abordagens. (Razzano, 2003) utiliza a técnica de transmissão adaptativa, onde ocorre um controle dos dados trafegados, de acordo com a necessidade. Isso acontece porque quando o *throughput* numa conexão é muito alto, a comunicação fica mais suscetível a erros. (Razzano, 2003) utiliza a lógica *fuzzy* para realizar o controle do tráfego de dados, para que se possa ter o domínio das ações apoiada em uma base do conhecimento e de dados mensurados previamente. Assim, a partir das experiências adquiridas pelo sistema, pode se controlar o tráfego de dados e com isso, otimizar o consumo de energia.

Em (Prasithsangaree, 2003) é realizada uma análise comparativa entre o algoritmo RC4 e o AES, onde são avaliados os seus impactos no consumo de energia. São observadas variáveis que estão sendo manipuladas (como o tamanho da chave e o tamanho do pacote a ser criptografado) e a partir disso, foi notado que o RC4 apresentava-se mais rápido e com menor consumo de energia quando se consideravam pacotes maiores. Em contrapartida, o AES consome menos energia quando são manipulados pacotes de tamanhos menores.

Em (Protlapally, 2003) são avaliados os impactos de variáveis de segurança no consumo de energia, realizando comparações entre diversos algoritmos, em que, alterando suas variáveis, podem interferir na utilização de recursos de bateria. Tipo de criptografia, tipo de algoritmo, tamanho da chave e utilização de uma camada de autenticação são mensurados, possibilitando que sejam confrontadas várias abordagens e sua influência na bateria do dispositivo móvel.

Em (Krintz, 2004) foi verificada a utilização dos recursos de bateria, visando fazer a previsão do consumo de uma determinada aplicação. Para realizar a previsão de consumo, foi determinada uma arquitetura na qual são realizados os testes, que integrados com *benchmarks*, proporciona antever a estimativa de consumo.

3. Metodologia utilizada

O ponto chave é encontrar um algoritmo que garanta o mínimo de segurança aos dados trafegados, sem provocar um consumo elevado de bateria, encontrando então, um ponto de equilíbrio na relação consumo x segurança. Segundo (Prasithsangaree, 2003), a criptografia de apenas 13,6 Kb de dados utilizando o algoritmo Blowfish (com 32 bits) em um handheld, cerca de 75% de sua bateria total pode ser consumida, enquanto o RC4 é considerado um algoritmo econômico, usando 7 ciclos de RAM por byte gerado. Nesse contexto, o objetivo do presente trabalho é automatizar a escolha de um algoritmo de criptografia, tendo o equilíbrio com o gasto energético.

Os experimentos estão sendo realizados em um PDA (Personal Digital Assistant), com processador StrongARM 206MHZ, 48 Mb de memória e um cartão de 256Mb, utilizando uma bateria de lítio recarregável de 1000 mAh. Como sistema operacional, o dispositivo utiliza a distribuição Familiar Linux v0.7.2, a qual implementa o gerenciamento de bateria usando o *Hardware Abstraction Layer* (HAL) e exporta os dados da bateria para o sistema de arquivos no diretório /proc.

Uma vez determinada a arquitetura e o ambiente em que são baseados os testes, deve ser feita uma análise nos algoritmos de criptografia que serão considerados. Assim, é avaliado o comportamento de cada algoritmo observando as variáveis: tipo do algoritmo, tamanho de chave e complexidade do algoritmo, e que impactos podem provocar na desempenho da bateria. Ou seja, a partir da implementação de algoritmos (utilizando a *virtual machine* Blackdown) pode-se avaliar a maneira como cada um procede em seu processo de encriptação.

Para analisar o impacto de um algoritmo sobre o consumo de energia, um fator a ser medido é o tempo envolvido na cifragem. O tempo de encriptação representa o tempo que o processador estava cifrando um texto. Em (Russel, 1998) observa-se uma metodologia para mensurar a energia consumida (i) por uma determinada aplicação, onde T é o tempo de execução (cifragem) e P(t) é a potência em um instante, P_m representa a potência média e E uma estimativa da energia envolvida no processamento. Tal metodologia é de grande importância para realizar as medições de cada algoritmo e é utilizada para medir o consumo decorrente de um processamento.

$$E = \int_{to}^{to+T} P(t)dt \qquad Pm = \frac{1}{T}\int_{to}^{to+T} P(t)dt \qquad E = T * Pm \quad \text{(i)}$$

A utilização da lógica *fuzzy* no projeto concentra-se em duas variáveis: segurança e consumo de energia. Uma vez realizada a modelagem destas variáveis através de conceitos de inteligência artificial, poder-se-á obter um algoritmo que seja o equilíbrio entre elas.

No que tange a segurança, deve ser considerado o tamanho da chave. De forma isolada este fator não é uma garantia de segurança, porém, o seu ajuste correto pode influenciar diretamente na confiabilidade do processo de cifragem - dificultando o ataque por força bruta (Burnett, 2002). A partir desse fato, é realizado o processo de *fuzzyfication*, onde a função de pertinência varia entre 0 e 1 e o tamanho da chave variando entre 56 bits e 1024 bits (devendo se adequar de acordo com o algoritmo), podendo ser definidos níveis de segurança em cada caso.

Quanto ao consumo de energia, deve ser analisado quão custoso um algoritmo pode ser, dependendo dos seguintes fatores: tamanho da chave utilizada, do tipo de algoritmo e do volume de dados a ser protegido. Em (Prasithsangaree, 2003) foi observado, por exemplo, que um algoritmo pode ter sua eficiência alterada de acordo com o volume de dados a serem manipulados. Os *fuzzy sets* devem ser baseados na integração de sub-conjuntos *fuzzy* dos fatores anteriormente citados. Isso permite, que seja avaliado o consumo de energia, de acordo com o tipo de criptografia que está sendo utilizado, onde o *fuzzy set* de consumo varia de acordo com o resultado de (i).

A modelagem destas variáveis e sua conseqüente integração interagem com uma camada responsável pela tomada de decisões. Esta se responsabiliza pela definição dos níveis críticos de energia e avalia a validade do algoritmo em uma situação. Em (ii) se verifica como se integram tais variáveis, onde os fatores representam níveis de pertinência do respectivo *fuzzy set*. Assim, pode observar-se que o grande desafio é a obtenção adequada destes fatores, já que influenciam diretamente no resultado final.

$$validadeAlgoritmo = \frac{(fator1 * tamanhoArquivo) * (fator2 * tamanhoChave)}{(fator3 * energiaDisponivel) * (fator4 * previsaoConsumo)} \quad \text{(ii)}$$

Dessa maneira, dependendo da capacidade energética disponível deve ser escolhido um algoritmo adequado. Isso porque cada algoritmo possui um comportamento no que tange o consumo de energia (Protlapally, 2003) e dependendo da carga energética disponível, poderá ser escolhido um algoritmo que satisfaça tal situação. Logo, utilizando técnicas de inteligência artificial, garante-se o equilíbrio entre segurança e utilização de recursos de bateria.

4. Conclusões

Percebe-se que a relação entre criptografia e consumo de energia é um problema real, pois há dificuldade em estabelecer de forma precisa o equilíbrio entre elas (devido a dependência de fatores subjetivos e abstratos). Para isso, a lógica *fuzzy* é de grande utilidade, já que serve para mapear conceitos para representações numéricas, garantindo maior precisão sobre uma definição.

Nesse contexto se insere o presente trabalho, uma vez que a integração de conceitos de inteligência artificial agregados a metodologias de consumo de energia, podem ser úteis para maximizar os níveis de segurança em dispositivos móveis, sem afetar de forma tão incisiva sobre os recursos de bateria.

Referências bibliográficas

RUSSEL, S.; NORVIG, P. **Artificial Intelligence: A Modern Approach.** Prentice Hall, 1995

JORSTAD, N. **Cryptographic Algorithms Metrics** Institute for Defense Analyses Science and Technology Division, 1997.

LI, Z.; XU, R. **Energy impact of secure computation on a handheld device.** Department of Computer Sciences, Purdue University – 2003.

PROTLAPALLY, N. ; RAVI, S. ; RAGHUNATHAN,A. ; JHA, N. **Analyzing the energy consumption of security protocols.** Proceedings of International Symposium on Low Power Eletronics and Design, 2003.

RAZZANO, G. **An efficient power saving mechanism for Wireless LAN.** Proceedings of the Eighth IEEE International Symposium on Computers and Communication – 2003.

PRASITHSANGAREE, P. ; KRISHNAMURTHY, P. **Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs.** Telecommunications Program. University of Pittsburgh, 2003.

BURNETT, S. *et al*. **Criptografia e segurança – Guia official RSA**. Editor Campus, 2002.

RUSSEL, J.; JACOME, M. **Sotware Power Estimation and Optimization or High Performance, 32-bit Embedded Processors**. Proceedings of International Conference on Computer Design, 1998.

KRINTZ, C. *et al*. **Application-level Prediction of Battery Dissipation**. Computer Science Department - University of California, 2004.