Avaliação de Desempenho de um Protocolo de Segurança para Sistemas RFID

Matheus A. Cavalcante[1] e Marcelo P. Sousa[12]
[1]Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), Campina Grande, PB, Brasil,
[2]Universidade Federal de Campina Grande (UFCG), Campina Grande, PB, Brasil.
E-mail: suehtamacv@gmail.com, marcelo.portela@ieee.org

I. Introdução

A tecnologia de Identificação por Rádio Frequência (RFID – *Radio Frequency Identification*) permite a comunicação dos dados de identificação de algum elemento usando ondas eletromagnéticas. Os dados estão armazenados em uma etiqueta RFID (*tag*), anexadas aos itens [1]. Conforme o custo das etiquetas reduz, o RFID torna-se popular. Sistemas como este são utilizados em pedágios automatizados, identificação de pacientes em hospitais, identificação animal, logística de transporte, manuseio e estocagem de produtos, etc.

Em 1999, o *Massachussets Institute of Technology* (MIT) idealizou uma nova possibilidade para as etiquetas RFID. Em vez de armazenar vários dados na etiqueta, o que requer mais memória, ela poderia armazenar apenas um identificador universal por meio do qual os dados do objeto seriam encontrados em bancos de dados disponíveis na Internet. Depois desta concepção, o uso do RFID tem sido difundido e adotado por empresas renomadas, como o Walmart, Gillete e Best Buy [2].

O expressivo investimento em pesquisa e desenvolvimento de tecnologias RFID pode auferir benefícios de natureza tática às empresas. No varejo, o uso de RFID pode proporcionar diversas melhorias, inclusive aumento do faturamento e menores custos de distribuição e operação, pois a aplicação de tais sistemas proveem melhor planejamento de promoções e reduções dos custos logísticos [1]. Alguns autores afirmam inclusive que a tecnologia RFID pode chegar a substituir os defasados códigos de barra (*barcode*). Com menores tempos de leitura que os estes, redução dos erros de leitura e escrita, maior vida útil e possibilidade de reutilização das etiquetas, há a ideia clara que os sistemas RFID são preferíveis em relação aos *barcode*. Entretanto, o ainda alto custo das etiquetas suporta também a noção de sistemas híbridos, usando RFID e código de barras ao mesmo tempo [3].

Com essa tecnologia, a princípio, é possível ler a etiqueta fixada em um determinado objeto mesmo que este esteja acondicionado dentro de uma bolsa, por exemplo. Essa leitura poderia ser realizada sem autorização ou até mesmo sem o conhecimento do proprietário do objeto, caracterizando uma invasão de privacidade [4].

Em sistemas RFID, o impacto dos riscos de invasão de privacidade podem ser diminuídos por meio da redução de dados sigilosos das etiquetas, controle do acesso físico, ou por blindagem eletromagnética. A segurança da informação gravada na etiqueta de RFID também tem motivado o desenvolvimento de protocolos com este objetivo [5]. Para garantir a segurança e a integridade dos dados transmitidos em sistemas RFID, os recursos tecnológicos adequados devem ser incorporados em tais dispositivos, de modo a garantir a privacidade dos dados e autenticação.

A necessidade de um baixo consumo de energia é primordial em sistemas RFID. Os sistemas ativos, que são providos de bateria, devem prolongar o tempo de vida desta de modo a estender seu tempo de operação. Os sistemas criptográficos comuns consomem muita energia e muitos ciclos de processamento, de modo que não são elegíveis para a inclusão em uma etiqueta RFID. Portanto, outras alternativas têm sido pesquisadas, entre elas a utilização de modulação pseudoaleatória [6].

A modulação é uma técnica que altera um ou mais parâmetros de uma portadora, com base no sinal mensagem de modo a viabilizar sua transmissão por um canal de comunicações. Se apenas o transmissor das informações, implementado na forma da etiqueta, e o receptor dos dados relatados - o leitor RFID - conhecerem o esquema de modulação para a transmissão correspondente, o invasor percebe uma dificuldade expressiva em demodular corretamente o conjunto de dados envolvidos no processo. Desse modo, as diferentes escolhas por esquemas de modulação é pseudoaleatória para o transmissor e receptor, mas é completamente aleatória do ponto de vista do invasor.

II. Modulação Pseudoaleatória

Neste artigo, os autores implementaram os fundamentos desenvolvidos em [5] e [6], por meio do desenvolvimento de um método de modulação que usa um gerador de números pseudoaleatórios (GNP) para modular o sinal, de forma que apenas o transmissor e o receptor sabem qual esquema de modulação está sendo usado no momento. Um invasor hipotético tentaria demodular o sinal sempre em um esquema fixo de modulação, e teria uma taxa de acerto do sinal próxima a 50%.

Para simular o sistema de modulação pseudoaleatória foi usado o programa *Octave 3.2.4*, devido ao mesmo ser *open-source* e ter uma variedade de recursos suficiente para as simulações necessárias. A ferramenta GNP usada foi a *Mersenne Twister*, pois este é um método bastante utilizado, criado em 1997, que passa por vários testes de "aleatoriedade" e que já é implementado por padrão no Octave.

Uma propriedade dos GNP é que, com a utilização de uma semente de geração de números aleatórios comum entre transmissor e receptor, as sequências pseudoaleatórias geradas também coincidem entre transmissor e receptor. Desse modo a aleatoriedade se torna verdadeira apenas do ponto de vista do invasor, que não conhece a semente e não consegue perceber um padrão na sequência.

Após um ciclo de geração de um novo número pseudoaleatório, há uma regra de decisão no código do modulador. Se o número é menor do que 0.5, o sinal digital é modulado em amplitude (*Amplitude Shift Keying – ASK*) [7]. Senão, o sinal digital é modulado em frequência (*Frequency Shift Keying – FSK*). A operação do demodulador, no leitor RFID destino, é bastante análoga. Já o invasor não conhece qual é o esquema de modulação utilizado e, na metodologia utilizada neste artigo, sempre tenta demodular apenas em ASK ou FSK. Nestas simulações foi considerado que o invasor sempre demodula em ASK, desconsiderando assim quaisquer variações da frequência do sinal modulado.

III. Avaliação de Desempenho

Pela análise dos resultados, verifica-se que o sinal modulado não parece guardar nenhuma relação óbvia com o sinal digital. Mesmo assim o leitor RFID destino consegue recuperar o sinal completamente, supondo um meio de transmissão ideal sem qualquer ruído. Já o sinal recuperado pelo invasor é bastante diferente do sinal original.

Ao simular o comportamento do invasor na análise de um sinal digital de 720 bits de comprimento, conforme esperado verificou-se que a frequência de acerto do mesmo varia de acordo com a semente do GNP. Para diminuir a influência da semente do GNP, foram realizadas dez simulações usando sementes diferentes e foi verificado que a média aritmética destas taxas aproxima-se do valor esperado de 50%. Os dados das experiências, a média aritmética ($\bar{x}$) e o desvio-padrão (σ) podem ser encontrados na Tabela I.

TABELA I

Taxa de acerto do invasor em função da semente do gerador de números pseudoaleatórios.

Semente do Gerador	Taxa de Acerto do Invasor
0	49,7%
1	48,3%
2	50,1%
3	50,8%
4	48,9%
5	51,7%
6	51,1%
7	52,9%
8	47,4%
9	51,1%
$\bar{x}$	**50,2%**
σ	**2,49**

Uma vez que o desvio-padrão é uma medida de dispersão relativa à média, o desvio-padrão pode ser considerado "grande" ou "pequeno" dependendo da ordem de grandeza dos valores. Assim, uma análise estatística melhor pode ser realizada por meio do coeficiente de variação c_v, que é definido como a razão do desvio-padrão pela média aritmética. O experimento com menor coeficiente de variação é mais preciso [8]. O valor coeficiente de variação obtido foi $c_v = 4,9\%$, que é razoavelmente baixo e demonstra que as taxas de acerto do invasor estão pouco dispersas e realmente se aproximam da média de $50,2\%$.

IV. Conclusão

Os resultados do modulador pseudoaleatório indicam valores promissores para a segurança do sinal, visto que ao menos em teoria o invasor não pode saber qual é a semente do GNP e não tem nenhuma forma óbvia de descobrir. Como o invasor não tem acesso aos números gerados, quaisquer algoritmos que tentem encontrar a semente do GNP são desconsiderados. Mesmo que o invasor conseguisse acesso aos números, as mensagens são curtas demais para que tais algoritmos sejam eficazes [6]. Caso uma nova semente seja usada a cada troca de mensagens, o modulador se torna ainda mais seguro.

Os resultados obtidos são coerentes com outros obtidos na literatura. Entretanto, ainda é preciso analisar se o invasor não conseguiria deduzir o sinal digital quando códigos de paridade fossem inseridos no sistema, ou ainda como as sementes do GNP seriam armazenadas na etiqueta.

A inclusão do comportamento de perda em pequena escala, como o desvanecimento do sinal, assim como do ruído aditivo dos componentes, está prevista para a simulação sobre um cenário de propagação mais real. Além disso, por se tratar de sistemas em que a economia de energia é um aspecto crítico, os autores pretendem avaliar o desempenho relativo ao consumo de energia do sistema e testar a relação de compromisso frente à robustez do esquema de segurança proposto.

Agradecimentos

Os autores agradecem ao CNPq e ao IFPB.

Referências

[1] M. C. Pedroso, R. Zwicker and C. A. d. Souza. "Adoção de RFID no Brasil: um estudo exploratório". *RAM. Revista de Administração Mackenzie*, vol. 10, pp. 12 – 36, 02 2009.

[2] M. Roberti. "The History of RFID Technology". *RFID Journal*, 2006.

[3] G. R. T. White, G. Gardiner, G. Prabhakar and A. A. Razak. "A Comparison of Barcoding and RFID Technologies in Pratice". *Journal of Information, Information Technology, and Organizations*, vol. 2, 2007.

[4] T. Karygiannis, B. Eydt, G. Barber, L. Bunn and T. Phillips. *Guidelines for Securing Radio Frequency Identification (RFID) Systems*. National Institute of Standarts and Technology, 2007.

[5] M. V. C. Rodrigues. "Segurança de Sistemas RFID com Modulação Aleatória". Master's thesis, Universidade Federal de Campina Grande, 2010.

[6] B. B. Albert, F. M. Assis, M. V. C. Rodrigues and S. Tedjini. "Perfomance Analysis of a Random Modulation Privacy Algorithm". In *Wireless Systems International Meeting*, 2010.

[7] M. S. Alencar. *Telefonia Celular Digital*. Érica, 2004.

[8] D. Mohallem, M. Tavares, P. Silva, E. Guimarães and R. Freitas. "Avaliação do coeficiente de variação como medida da precisão em experimentos com frangos de corte". *Arquivo Brasileiro de Medicina Veterinária e Zootecnia*, vol. 60, 04 2008.