RFID - *Radio Frequency Identification*

Rafael Perazzo Barbosa Mota
NUSP: 5060192

monografia desenvolvida
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
a disciplina MAC5743
de
Computação Móvel

Programa: Pós-graduação em ciência da computação
Professor: Prof. Dr. Alfredo Goldman

-

São Paulo, junho de 2012

Resumo

Identificação por radiofrequencia (RFID - *Radio Frequency identification*) é um termo genérico que é usado para descrever um sistema que transmite a identificação (sob a forma de um código, denominado código EPC) de um objeto ou pessoa, sem fios, utilizando ondas de rádio. Ao contrário da tecnologia de código de barras, a tecnologia RFID não requer contato ou linha de visão para a comunicação. Dados de etiquetas RFID podem ser lidas através de materiais utilizados pelas pessoas como a roupa do corpo, bolsas entre outros. A finalidade de um sistema RFID é o de permitir que os dados sejam transmitidos por um dispositivo portátil, chamados de etiqueta (ou tag), que é lido por um leitor RFID e processado de acordo com as necessidades de uma aplicação particular. Os dados transmitidos pela etiqueta pode fornecer identificação ou localização de informações, ou informações específicas sobre o produto marcado, como o preço, cor, data de compra, entre outras. A tecnologia RFID vem sendo utilizada por milhares de empresas ao redor do planeta e rapidamente ganhou atenção devido à sua grande capacidade de se adaptar aos mais diversos cenários de aplicações. Neste trabalho apresentamos o funcionamento da tecnologia, principais aplicações e alguns problemas de segurança e privacidade que envolvem sua utilização.

Palavras-chave: Computação móvel, Computação ubíqua, segurança, privacidade.

Abstract

MOTA, R. P. B. **RFID - *Radio Frequency Identification***. 2012. 21 f. Monografia (Disciplina) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2012.

Radiofrequency Identification (RFID) is a generic term that is used to describe a system that transmits the identity (in the form of a code, called EPC) of an object or person wirelessly using radio waves. Unlike the bar code technology, RFID technology does not require contact or line of sight for communication. RFID tag data can be read through materials used by people like the clothes, bags and more. The purpose of an RFID system is to enable data to be transmitted by a portable device, called the label (or tag) that is readable by an RFID reader and processed according to the needs of a particular application. Data transmitted by the tag may provide identification or location information, or specific information about the product tagged, such as price, color, date of purchase, among others. RFID technology has been used by thousands of companies around the globe and quickly gained attention because of its great capacity to adapt to various application scenarios. This text presents the technology, some main applications, security and privacy issues surrounding its use.

Keywords: Mobile Computing, Ubiquous Computing, security and privacy.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Identificação por Radiofreqüência (RFID *Radio Frequency Identification*) é uma tecnologia que utiliza ondas de radiofrequência para transmissão de dados. O recurso existe há muito tempo, como uma forma de leitura remota de dados (de identificação), armazenados em objetos, anexados a bens ou seres vivos. Sua primeira grande aplicação deu-se durante a Segunda Guerra Mundial, quando foi usada pelas forças britânicas para identificar inimigos e amigos respondendo ou não a pedidos de identificação por meio de ondas de rádio (Want, 2006).

Foram necessários mais de trinta anos de evolução da eletrônica, levando à associação da RFID a técnicas digitais de tratamento da informação, até que se chegasse à possibilidade da sua ampla disseminação. Isso envolve componentes eletrônicos, microeletrônicos e softwares especializados, compondo um sistema de identificação digital (Sarma *et al.*, 2003).

As potênciais aplicações para sistemas de RFID são inúmeras, variando desde a simples identificação remota de objetos até avançadas utilizações em cadeia de suprimentos, segurança e rastreamento de objetos (Ahson e Ilyas, 2008).

A principal vantagem do uso da tecnologia RFID é a realização da leitura sem o contato direto do leitor com o tag. É possível, por exemplo, colocar a tag dentro de um produto e realizar a leitura sem ter que desempacotá-lo. O tempo de resposta é baixíssimo tornando-se uma boa solução

em processos produtivos em que a tag encontra-se em movimento. Comparado com o sistema de leitura de código de barras a tecnologia aqui descrita apresenta inúmeras vantagens como o seu formato, segurança, manutenção e utilização. A função desta tecnologia tem caráter primário já que transmite os dados para uma leitora que já processa as informações [1].

O sistema é formado basicamente por três componentes chaves: o leitor; as tags (ou etiquetas) que são fabricadas nos mais diversos formatos e custos de fabricação); e uma aplicação externa. O leitor faz requisições às tags que, por sua vez, enviam a resposta. Recebida a informação desejada, o leitor pode ainda interagir com uma aplicação externa, geralmente um *middleware* específico Ahson e Ilyas (2008).

1.1 Objetivos

O objetivo deste trabalho é apresentar a tecnologia RFID, mecanismos de funcionamento, suas potênciais aplicações, problemas relacionados à segurança e privacidade, algumas soluções da literatura, assim como as possibilidades de trabalhos futuros na área.

1.2 Organização do Trabalho

No Capítulo 2, apresentamos os conceitos fundamentais da tecnologia. No capítulo 3 apresentamos as principais aplicações. O capítulo 4 apresenta os principais problemas de segurança e privacidade. Finalmente o Capítulo 5 discutimos algumas conclusões obtidas no desenvolvimento do trabalho.

[1] http://www.theriontec.com.br/pagina/rfid-identificacao-por-radio-frequencia

Capítulo 2

O sistema RFID

2.1 Componentes de um Sistema RFID

Um sistema RFID é formado por 3 componentes básicos (Want, 2006) (Verdult, 2008)

- *Transponder* ou tag RFID: localizada no objeto a ser identificado, armazenando o código de identificação.
- *Transceiver* ou leitor RFID: responsável pela leitura/escrita na tag.
- *Middleware* ou banco de dados: responsável pelo processamento da informação obtida pelo leitor.

A Figura 2.1 ilustra um sistema RFID genérico.

2.1.1 Tags RFID

Tags RFID (*Transponders*) consistem de um microchip que armazena os dados e um elemento de acoplamento, tal como uma antena, utilizada para a comunicação através da radiofrequencia. A Figura 2.2 ilustra um exemplo de tag.

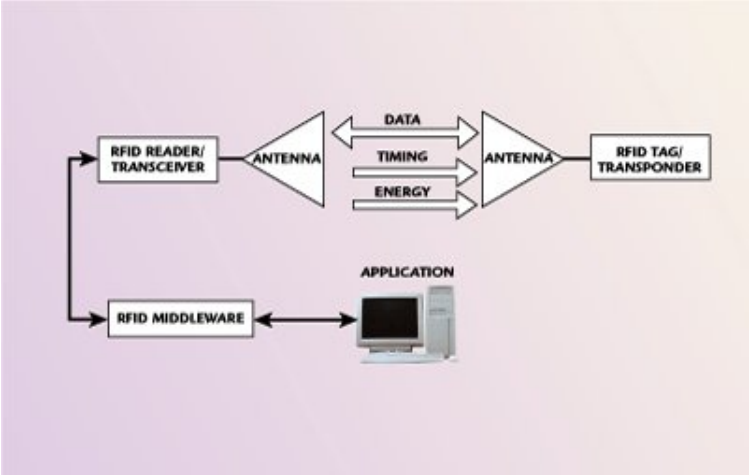

Figura 2.1: *O sistema RFID*

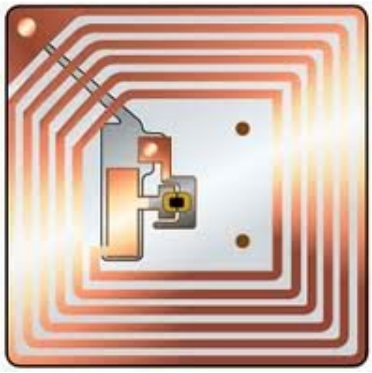

Figura 2.2: *Tag RFID*

Podem ser classificadas conforme as seguintes características:

- Energização
- Leitura/Escrita
- Frequência de operação

A classificação de acordo com o tipo de energização classifica as tags em ativas, semi-passivas e passivas. Tags ativas contêm uma fonte de energia própria, como uma bateria, possuindo a habilidade de iniciar sua própria comunicação com o leitor como também com outras tags. Tags semi-passivas possuem bateria, mas podem apenas responder à transmissões que cheguem até elas. Tags passivas recebem toda energia através do leitor e não podem iniciar nenhuma comunicação por iniciativa própria. Para oferecer uma analogia de como o processo de energização passiva funciona, devemos pensar que os leitores ”gritam” para as tags passivas, e depois extraem os dados resultan-

tes do ”eco”. Tags passivas são completamente inativas na ausência de umv leitor (Knospe e Pohl, 2004). As etiquetas passivas não utilizam uma fonte de energia própria, em vez disso eles capturam energia eletromagnética produzida pelo leitor através de indução magnética e utilizam essa energia para enviar sinais para as antenas (ver Figura 2.3).

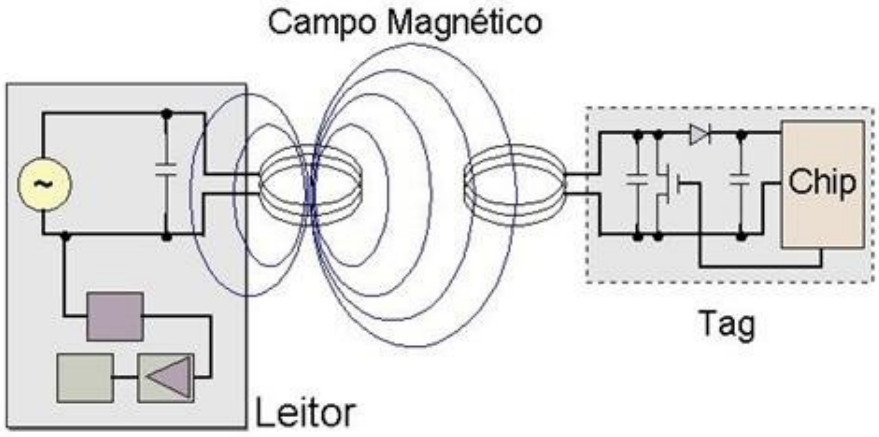

Figura 2.3: *Energização de uma tag passiva*

Outra forma de classificar as tags é de acordo com as capacidades de leitura/escrita EPCglobal (2004)

- Classe 1: são etiquetas onde grava-se uma vez e lê-se várias (*Write once ? read many*). A idéia principal é que os dados são gravados apenas uma vez. São geralmente usadas para a simples identificação de produtos ou em cartões de acesso. São o tipo de etiquetas mais utilizadas no mundo inteiro devido a sua especificação estar completa e operacional, além de possuir custos menores em relação às demais.
- Classe 2: permitem tanto leitura quanto gravação (várias vezes). Tipicamente possuem mais memória e capacidade de gerar logs.
- Classe 3: também possuem capacidade de leitura e escrita mas também possuem sensores acoplados. Possuem circuitos para registrar temperatura, pressão entre outros.
- Classe 4: são as mais sofisticadas que além de possuírem todos os recursos oferecidos pelas Classes anteriores, estas possuem capacidade de iniciar comunicação com outras tags ou dispositivos com ou sem a presença de um leitor. Para operar independentemente do leitor estas tags precisam possuir bateria própria Roberts (2006).

Já a classificação relacionada a frequência de operação caracteriza as tags da seguinte forma

(EPCglobal, 2004):

- Frequência menos do que 135Khz: São tags passivas, de baixo custo, baixa velocidade de leitura e baixos níveis de energia. Temos como exemplos a utilização em fechaduras de carros, e controle de acesso.
- Frequência de 13.56Mhz: São geralmente passivas, também de baixo custo, e velocidade de leitura um pouco maior. São bastante utilizadas em controle de acesso e *smartcards*.
- Frequência de 860-930Mhz: Podem ser ativas ou passivas e possuem custo mais elevado que as anteriores, porém com velocidade de leitura mais alta. Cadeias de suprimento e estoques são os principais exemplos de sua utilização.
- 2.45Ghz: São ativas, possuem altíssima velocidade de leitura, custo elevado e são utilizadas geralmente em objetos de alto valor agregado.

As ondas de radiofreqüência variam de 30Khz a 300Ghz. Apenas algumas faixas de freqüências estão disponíveis para sistemas RFID. Certas faixas de freqüências adequam-se melhor a aplicações específicas. Sistemas RFID que operam nas faixas de 13.56Mhz e entre 860-930Mhz são os mais disseminados e utilizados pela industria. A freqüência de 13.56Mhz é bastante comum devido a disseminação dos cartões inteligentes (*smartcards*) baseados na tecnologia RFID. Já a freqüência entre 860-930Mhz são muito práticas para utilização em controle de estoque e cadeia de suprimentos pois oferece um bom alcance (alguns metros) como também possui o recurso da leitura de várias tags em alta velocidade de leitura.

2.1.2 Leitores RFID

Os leitores são os dispositivos que consultam as tags por seus dados, através de uma interface de radiofrequência. A comunicação com as tags além de envolver a requisição dos dados das tags pode ainda incluir comandos de escrita de dados na tag, se esta permitir (Ranasinghe *et al.*, 2004) (Weis, 2003). Leitores possuem sua própria fonte de energia, capacidade de processamento e uma antena de comunicação. Podem ser dispositivos a parte, ou seja, com funcionalidade apenas de leitor RFID, podem aparecer acoplados a outros dispositivos como *smartphones*, gps ou mesmo aparecerem fixos

em prateleiras inteligentes (Knospe e Pohl, 2004). A Figura 2.4 ilustra um exemplo de leitor RFID portátil e sem acoplamento com outro dispositivo.

Figura 2.4: *Exemplo de leitor RFID portátil*

No contexto global do sistema RFID, os leitores são posicionados como a entidade central, pois se localizam no centro da comunicação, entre as tags e o *middleware*.

Outro ponto importante relacionado aos leitore RFID está relacionado aos canais de comunicação: chama-se de canal *forward* o canal leitor para tag e de *backward* o canal tag para leitor. O alcance de ambos os canais depende dos tipos de dispositivos utilizados, e podem variar de alguns centímetros a vários metros de distância (Knospe e Pohl, 2004). Independente dos dispositivos utilizados no sistema, sempre existirá a chamada assimetria entre os canais *forward* e *backward*, ou seja, teremos que o canal forward terá um alcance bem maior que o canal backward, o que gera problemas de segurança que serão discutidos Capítulo 4 (Juels, 2006).

Se existem mais de uma tag dentro do alcance do leitor, um mecanismo anti-colisão é necessário. Um exemplo de algoritmo determinístico simples é o percurso em árvore binária (*binary tree walking*) onde o leitor questionará todas as tags na vizinhança para o próximo bit de seus identificadores. Se dois valores diferentes de bits forem transmitidos de um conjunto de tags, o leitor será capaz de detectar a colisão. O leitor então fará uma difusão de um bit indicando se tags que enviaram um 0 ou um 1 devem continuar. Essencialmente, o leitor escolhe uma ramificação da árvore binária de valores de identificadores. Tags que não se enquadram na escolha do leitor não continuarão participando do protocolo. À medida que o leitor continua a percorrer as ramificações da árvore binária, poucas

tags continuarão operando. Assim no fim do algoritmo apenas uma tag estará respondendo. Este processo de endereçar e isolar uma única tag pode ser chamado de **singularização** (Sarma *et al.*, 2003).

2.1.3 *Middleware*

Middleware é um termo genérico utilizado para descrever o *software* que está entre o leitor e as aplicações empresariais (Weis, 2003). As empresas necessitam de servidores para executar o middleware dentro de um centro de distribuição, depósito, instalação de produção ou aplicação específica. Esses servidores são chamados servidores de borda, porque eles estão perto da borda da rede em que o mundo digital ou eletrônico se encontra com o mundo real. Os servidores de borda são servidores comuns e normalmente não possuem nenhum hardware especial. Conectam aos leitores usando serial ou Universal Serial Bus (USB).

Segundo Ahson e Ilyas (2008) e Weis (2003), um sistema RFID só torna-se efetivamente completo e utilizável na prática, quando os leitores interagem de alguma maneira com uma aplicação externa. Devido à flexibilidade desta entidade, temos que sistemas computacionais independentes podem ser construídas por qualquer pessoa para atender as necessidades da aplicação específica. Os dados armazenados geralmente incluem nome do produto, fabricante, validade, chave de criptografia entre outros detalhes escolhidos de acordo com aplicação do sistema.

Capítulo 3

Aplicações

A tecnologia RFID pode ser aplicada em inúmeros cenários e situações conforme alguns exemplos mostrados a seguir (Ahson e Ilyas, 2008)

- **Controle de acesso (segurança)**: No travamento e destravamento de veículos as chaves com tags são detectadas à distância, liberando as travas das portas e a partida do veículo. O mesmo princípio é utilizado para controle de acesso a prédios e áreas restritas. A Figura 3.1 ilustra a aplicação.

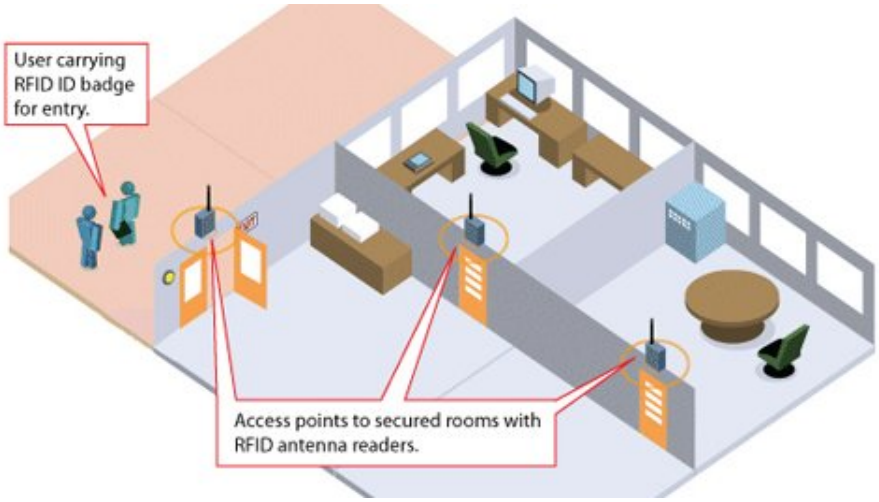

Figura 3.1: *Controle de Acesso com RFID*

- **Aeroportos**: A movimentação de bagagens em aeroportos pode ser beneficiada fazendo as bagagens serem etiquetadas com tags contendo o número do vôo, o nome do passageiro e um

número seqüencial que as identificam. São rastreadas durante a sua colocação nas aeronaves, minimizando a ocorrência de bagagens perdidas. A Figura 3.2 mostra a aplicação da tecnologia em Hong Kong.

Figura 3.2: *RFID em bagagens - Hong Kong*

- **Controle de estoques**: Já o controle de estoques (ver Figura 3.3 faz com que todos os itens sejam identificados, sendo possível detectar a saída de um item do estoque. O software de controle notifica a remoção do item, associada à identificação do funcionário e ao horário em que isso aconteceu. Promove, também, uma varredura eletromagnética para leitura de todos os itens remanescentes no estoque. Se for o caso, efetua um comando para reposição.

Figura 3.3: *Controle de estoques*

- **Rastreamento animal**: O rastreamento animal, muito utilizado na pecuária com a colocação

de tags em animais permite que eles sejam identificados e associados a dados individuais e históricos de movimentação, sanidade, administração de medicamentos, etc. É uma aplicação bastante utilizada no Brasil (ver Figura 3.4).

Figura 3.4: *Rastreamento animal*

- **Cadeia de suprimentos**: No controle da cadeia de suprimentos a identificação de embalagens pelos fornecedores permite a uma empresa distribuidora ou varejista um controle mais preciso e ágil de sua cadeia de fornecedores, melhorando a gestão dos estoques e reduzindo perdas. É um dos campos mais promissores para utilização da tecnologia.

- **Aplicações médicas e hospitalares**: Permite a identificação dos pacientes através de tags implantadas por baixo da pele (Figura 3.5. Médicos e outros profissionais de saúde podem rapidamente através de leitores portáteis, obter todas as informações sobre os pacientes, em diversos cenários como internações, cirurgias, consulta de prontuário entre outras.

Figura 3.5: *Tag subcutânea*

- **Bibliotecas**: Utiliza-se para identificação do acervo, possibilitando leitura e rastreamento dos exemplares físicos das obras, agilizando também os processos de emprestimo, devolução, renovação e segurança do acervo, conforme apresentado na Figura 3.6.

Figura 3.6: *Utilização em biblioteca*

- **Supermercados**: Permite que os consumidores passem com o carrinho de compras (os produtos devem estar etiquetados com tags) pelo caixa equipado com um leitor, que automaticamente faz a leitura de todos os itens informando rapidamente o valor da compra. Torna a ida a um supermercado ou loja de compras uma tarefa rápida e eficiente. A Figura 3.7 mostra um esboço de um supermercado do "futuro" [1].

Figura 3.7: *Supermercado do futuro*

[1] Em vários países desenvolvidos já existem este tipo de supermercados

- **Prateleiras inteligentes**: Este cenário de aplicação (Figura 3.8) funciona de forma similar ao controle de estoques, sendo que aplicado de forma local, em uma loja por exemplo. Quando um item é retirado da prateleira, o leitor informa imediatamente ao *middleware* que o item foi removido. O mesmo ocorre quando o item é devolvido. Em resumo, torna muito ágil tarefas até pouco tempo cansativas.

Figura 3.8: *Prateleira inteligente*

- **Veículos**: A tecnologia permite agilidade em pagamento de pedágios e estacionamentos de shoppings. Através de uma tag fixada no para-brisa, o usuário tem acesso a pontos que possuem um leitor instalado e este(o leitor) faz esta leitura e abre a cancela automaticamente (conforme Figura 3.9.

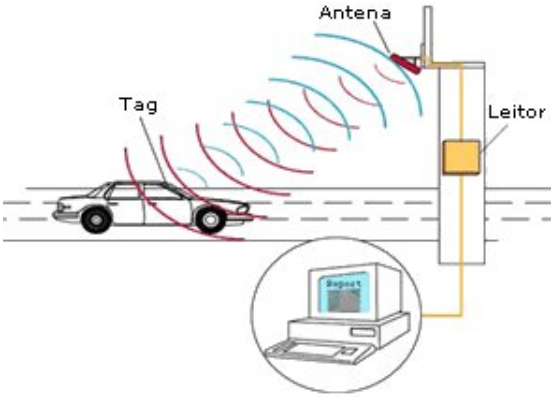

Figura 3.9: *Controle de Acesso de veículos com RFID*

Os exemplos listados acima são apenas os principais cenários que podem se beneficiar da tecnologia, que é bastante flexível, podendo se adaptar a diversas outras aplicações.

Capítulo 4

Segurança e privacidade

Segundo o dicionário AURÉLIO, informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza. A segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Tanenbaum (2003) caracteriza segurança pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

Um sistema seguro, segundo Stallings (2002) e Tanenbaum (2003) deve garantir as seguintes características:

- **privacidade**: A privacidade garante que ninguém está "farejando" o que está sendo transmitindo na rede (comunicação leitor-tag e tag-leitor) sem estar autorizado.
- **autenticação**: A autenticação garante que a origem da mensagem foi corretamente identificada, com a certeza de que a identificação não é falsa, ou seja, a origem é realmente quem diz ser.
- **integridade**: A integridade garante que o que foi transmitido não foi alterado, de forma nenhuma, durante a transmissão.
- **não repúdio**: O não-repúdio consiste no fato de requerer que nem o remetente nem o desti-

natário de uma mensagem sejam capazes de negar a mensagem, nem de negar que tenha sido enviada, nem negar que tenha sido recebida, se realmente isso tenha acontecido.

- **controle de acesso**: O Controle de Acesso requer que o acesso à informação possa ser controlado pela rede que contenha a informação. Algumas vezes, se quer dar acesso somente de leitura a um arquivo, ou no caso dos sistemas RFID, pode ser desejável que apenas leitores autorizados consultem o conteúdo das tags.

- **disponibilidade**: a disponibilidade requer que o sistema computacional esteja disponível para qualquer pessoa autorizada em qualquer momento que ela deseje

4.1 Principais problemas de segurança e privacidade em sistemas RFID

Segundo Ouafi (2012) e Erguler (2011) os grandes ganhos de eficiência oferecidos pelos sistemas RFID podem vir com um custo em segurança e privacidade. Vulnerabilidades como ataques físicos, plágio ou falsificação (*spoofing*), captura de tráfego, análise de tráfego e negação de serviço podem todas estar presentes nesses sistemas. E cada um destes riscos, conforme relatado por Sarma *et al.* (2003), pode afetar ambos os indivíduos e organizações . Até mesmo as mais modernas tags especificadas pela EPCGlobal, as chamadas Gen 2, EPCglobal (2004), não oferecem segurança adequada aos usuários. Na maioria dos casos, o custo de fabricação de tags com *hardware* de criptografia, é bastante elevado, invibializando a utilização da tecnologia em diversos cenários possíveis. A Tabela 4.1, resumida por Mota (2006), ilustra o cenário de problemas.

4.2 Algumas soluções propostas

Na literatura, diversas soluções foram propostas[1] para eliminar ou minimizar vários tipos de problemas relacionados à segurança e privacidade. Apresentaremos agora aquelas desenvolvidas pelos mais importantes pesquisadores da área (Erguler, 2011).

[1] http://www.avoine.net/rfid/

Tipo	Como funciona	Abordagem
Físico	O intruso pode realizar ataques físicos às tags.	Esquemas de segurança física de objetos, como contratação de seguranças, sistemas de câmeras, etc.
PLÁGIO ou FALSIFICAÇÃO (fabricação)	O intruso pode realizar consultas às tags e responder consultas a leitores legítimos.	Esquemas de autenticação e controle de acesso.
INTERCEPTAÇÃO (e modificação)	O intruso captura os quadros que trafegam no ar, também chamado de espionagem.	Esquemas de criptografia dos dados que são enviados entre as entidades leitor e tag.
NEGAÇÃO DE SERVIÇO (interrupção)	O intruso atrapalha as difusões interferindo nos sinais de radiofreqüência.	Muito difíceis de serem evitados, e por isso são bastante danosos.
PRIVACIDADE DE LOCALIZAÇÃO (RASTREAMENTO)	O intruso faz leituras nas tags que o usuário carrega podendo rastrear a localização do usuário.	Esquemas de autenticação e controle de acesso.

Tabela 4.1: *Principais problemas de segurança em sistemas RFID*

4.2.1 *Killing* tags

Esta abordagem permite que o leitor envie um comando *kill* para a tag que torna-se permanentemente inoperante. Como ”tags mortas” não podem ser reativadas, o processo de ”matar” a tag é uma medida altamente eficaz em termos de privacidade. As previsões de que as etiquetas RFID vão tornar-se predominantes em itens compras, os próprios estabelecimentos devem ”matar” as etiquetas RFID dos produtos comprados, para proteger privacidade do consumidor. Por exemplo, depois de passar com seu carrinho de supermercado através de um caixa automatizado e pagar a conta total, todas os produtos com tags RFID serão desativados no local (Elkhiyaoui *et al.*, 2012).

4.2.2 *Minimalist cryptography*

Juels (2004) propos um esquema de criptografia denominada ”minimalista”: Esta é uma solução baseada em pseudônimos pré-programados carregados pelas tags. Através da utilização de diferentes pseudônimos durante sessões diferentes de leituras, a tag evita o rastreamento por entidades não autorizadas. Já uma entidade autorizada tem acesso aos pseudônimos e pode realizar o rastreamento se for o caso. A proposta descreve um protocolo que possui propriedades de autenticação e privacidade, preocupando-se com as limitações do poder de computação e da capacidade de arma-

zenamento. Não envolve cálculos criptográficos intensivos e nem envolve a necessidade de aumento de recursos das tags.

4.2.3 Autenticação mútua

Fernando e Abawajy (2011) em seu trabalho abordaram o problema da segurança em sistemas RFID. Os mesmos desenvolveram e apresentaram um protocolo de segurança que permite autenticação mútua entre o leitor e a tag, bem como a comunicação segura dos dados de tag. O protocolo apresentado utiliza um método híbrido para fornecer segurança forte, assegurando os requisitos de recursos são baixos. Para este fim, emprega uma simples mistura de funções hash e operações de baixo custo, bit a bit. O protocolo garante a confidencialidade e integridade de todos os dados que estão sendo comunicados e permite a autenticação de confiança mútua entre as tags e leitores. O protocolo apresentado também é dito ser resistente a um grande número de ataques comuns.

Malek e Miri (2012) desenvolveu um protocolo de autenticação mútua entre tags e leitores, ou seja, ambas as entidades autenticam uma a outra. O protocolo proposto é baseado no sistema criptográfico publicado por McEliece (1978) com a diferença de que não é necessário que as tags armazenam matrizes esparssas, conforme o protocolo McEliece. Operações computacionais complexas são substituidas por operações binárias simples em vetores pequenos. A quantidade de memória necessária para as tags encaixa-se na utilização em etiquetas de baixo custo. Os leitores são os responsáveis pelas operações de encriptação e desencriptação envolvidas no protocolo McEliece. Após cada autenticação, o conteúdo das tags é disponibilizado e posteriormente a tag fica pronta para uma nova autenticação. Dessa forma, temos que o protocolo proposto assegura que apenas leitores autorizados possam consultas as tags, protegendo assim o sistema contra violação de privacidade.

Zhou *et al.* (2012) em sua publicação, também apresentam um protocolo de autenticação mútua baseado em criptografia com curvas elipticas para sistemas RFID. Considerando-se segurança e eficiencia entre as partes (tags e leitores), ambas não possuem a chave secreta em comum para compartilhar no protocolo, o que é considerada uma vantagem em relação a outros protocolos. OO protocolo proposto é densenvolvido para a minimização da computação nas tags. Os autores mostraram que o protocolo é escalável e apresentaram uma prova da confiabilidade do protocolo.

Capítulo 5

Conclusões

Este trabalho apresentou a tecnologia RFID, em termos gerais, na identificação de objetos. É uma tecnologia que está em crescimento contínuo, pois a cada dia aumenta o número de aplicações que fazem uso da mesma. Em países desenvolvidos o RFID já agiliza a vida de milhares de pessoas em aplicações como loja do futuro, cadeia de suprimentos, estoques entre várias outras. Foram apresentados também várias implicações da utilização da tecnologia relacionadas à segurança e privacidade assim como algumas soluções da literatura. Trata-se de um campo ainda aberto a novas investigações, pois busca-se cada vez mais diminuir os custos das tags e ao mesmo tempo tornar o sistema seguro e privativo.

5.1 Considerações Finais

Os sistemas RFID tornarão-se bastante presentes em um futuro próximo, o que levará as pessoas a pensar em um novo comportamento quanto consumidores e quanto cidadãos comuns. Este fato deve-se a ubiquidade da tecnologia, ou seja, a maioria das pessoas comuns utilizarão a tecnologia, sem mesmo saber que estão utilizando, gerando alguns problemas já citados relacionados à privacidade. No entanto prevemos que os benefícios serão bem maiores que os problemas.

Em relação às soluções propostas pela literatura para minimização de problemas de segurança

e privacidade, conclui-se que um esquema de autenticação mútua será provavelmente a melhor alternativa para resolver o problema, o que justifica uma grande quantidade de publicações recentes a respeito de diversos protocolos de autenticação, alguns dos quais apresentamos nesta monografia.

5.2 Sugestões para Pesquisas Futuras

Protocolos de comunicação que utilizem criptografia de baixo custo e autenticação mútua são temas que estão sendo bastante investigados, porém ainda longe de soluções ótimas. Dessa forma a pesquisa em segurança e privacidade de sistemas RFID é uma excelente área para novas investigações por tratar-se de um assunto vasto, e muito citada na literatura especializada.

Referências Bibliográficas

Ahson e Ilyas(2008) S. Ahson e M. Ilyas. *RFID handbook: applications, technology, security, and privacy*. CRC. Citado na pág. 1, 2, 8, 9

Elkhiyaoui *et al.*(2012) Kaoutar Elkhiyaoui, Erik-Oliver Blass e Refik Molva. T-MATCH: Privacy-preserving item matching for storage-only RFID tags. Em *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands. Citado na pág. 16

EPCglobal(2004) EPC EPCglobal. Radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860 mhz–960 mhz version 1.0. 9. *URL: http://www. epcglobalinc. org/standards*. Citado na pág. 5, 6, 15

Erguler(2011) Imran Erguler. *Security and Privacy Analysis of Authentication Protocols in RFID Systems*. Tese de Doutorado, Bogazici University, Bogazici University Electrical-Electronics Engineering, Istanbul, Turkey. Citado na pág. 15

Fernando e Abawajy(2011) Harinda Fernando e Jemal Abawajy. Mutual authentication protocol for networked RFID systems. Em *10th International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2011*, páginas 417–424. Citado na pág. 17

Juels(2006) A. Juels. Rfid security and privacy: A research survey. *Selected Areas in Communications, IEEE Journal on*, 24(2):381–394. Citado na pág. 7

Juels(2004) Ari Juels. Minimalist Cryptography for Low-Cost RFID Tags. Em Carlo Blundo e Stelvio Cimato, editors, *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, páginas 149–164, Amalfi, Italy. Springer. Citado na pág. 16

Knospe e Pohl(2004) H. Knospe e H. Pohl. Rfid security. *Information Security Technical Report*, 9(4):39–50. Citado na pág. 5, 7

Malek e Miri(2012) Behzad Malek e Ali Miri. Lightweight mutual RFID authentication. Em *IEEE International Conference on Communications – ICC2012*, Ottawa, Canada. Citado na pág. 17

McEliece(1978) R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116. Citado na pág. 17

Mota(2006) R.P.B. Mota. Extensões ao protocolo de comunicação epcglobal para tags classe 1 utilizando autenticação com criptografia de baixo custo para segurança em identificação por radiofreqüência. Dissertação de Mestrado, Universidade Federal de São Carlos, Bogazici University Electrical-Electronics Engineering, Istanbul, Turkey. Citado na pág. 15

Ouafi(2012) Khaled Ouafi. *Security and Privacy in RFID Systems*. Tese de Doutorado, EPFL, Lausanne, Switzerland. Citado na pág. 15

Ranasinghe *et al.***(2004)** D. Ranasinghe, D. Engels e P. Cole. Low-cost rfid systems: Confronting security and privacy. Em *Auto-ID labs research workshop*, páginas 54–77. Citeseer. Citado na pág. 6

Roberts(2006) C.M. Roberts. Radio frequency identification (rfid). *Computers & Security*, 25(1): 18–26. Citado na pág. 5

Sarma *et al.***(2003)** S. Sarma, S. Weis e D. Engels. Rfid systems and security and privacy implications. *Cryptographic Hardware and Embedded Systems-CHES 2002*, páginas 1–19. Citado na pág. 1, 8, 15

Stallings(2002) W. Stallings. *Wireless communications and networking*. Prentice Hall. Citado na pág. 14

Tanenbaum(2003) A. Tanenbaum. *Redes de Computadores, 4ª. edição traduzida, Editora Campus*. Elsevier. Citado na pág. 14

Verdult(2008) Roel Verdult. Security analysis of RFID tags. Dissertação de Mestrado, Radboud University Nijmegen. Citado na pág. 3

Want(2006) R. Want. An introduction to rfid technology. *Pervasive Computing, IEEE*, 5(1): 25–33. Citado na pág. 1, 3

Weis(2003) Stephen Weis. Security and Privacy in Radio-Frequency Identification Devices. Master thesis, Massachusetts Institute of Technology (MIT), MIT, Massachusetts, USA. Citado na pág. 6, 8

Zhou *et al.***(2012)** Jingxian Zhou, Yajian Zhou, Feng Xiao e Xinxin Niu. Mutual authentication protocol for mobile RFID systems. *Journal of Computational Information Systems*, 8(8):3261–3268. Citado na pág. 17