UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS APLICADAS E EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIAS EXATAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ASPECTOS TEÓRICOS DE SEGURANÇA EM RFID

Rio Tinto - PB

Novembro - 2018

ASPECTOS TEÓRICOS DE SEGURANÇA EM RFID

Autor: Rualyson Cavalcante Soares
Orientador: Prof. Dr. Augusto César Pereira da Silva Montalvão

Rio Tinto - PB
Novembro - 2018

ASPECTOS TEÓRICOS DE SEGURANÇA EM RFID

Monografia apresentada como parte dos requisitos para obtenção do título de Bacharel à banca examinadora no Curso de Bacharelado em Sistemas de Informação do Centro de Ciências Aplicadas e Educação (CCAE), Campus IV da Universidade Federal da Paraíba.

Orientador: Prof. Dr. Augusto César Pereira da Silva Montalvão

Dedico este trabalho aos meus pais, pessoas que admiro e amo, que sempre acreditaram em mim e me deram forças para não desistir.

AGRADECIMENTOS

Quero agradecer primeiramente a minha família, em especial, minha mãe Rogéria Cavalcante e meu pai Gilvan Soares que sempre acreditaram em mim.

Agradeço a minha namorada Lucrécia Barros, por estar sempre ao meu lado, por todo o carinho e compreensão, principalmente nos momentos de dificuldade ao longo do tempo.

Ao orientador deste trabalho, Augusto Montalvão, por ter acreditado em mim, pela paciência e atenção dedicada, pelo seu exemplo de dinamismo e trabalho, que é a maior lição que um professor pode dar a seu aluno.

A todos os colegas e amigos que fiz ao longo de minha graduação, alguns desses amigos para todos os momentos, amigos que com certeza levarei para o resto da vida.

Quero agradecer a todos os professores que eu tive nesses anos de graduação.

Agradeço aos amigos e amigas que sempre estiveram comigo, me apoiando, me ajudando quando necessário, e sempre torcendo por mim.

Agradeço também a todos que participaram, de uma forma ou de outra, desses anos de graduação.

RESUMO

Radio-Frequency IDentification (RFID) consiste em uma tecnologia de transmissão de dados sem fio por meio dos sinais de rádio. A tecnologia RFID vem se expandindo em diversas áreas distintas, principalmente em setores que buscam a automação dos dados. No entanto, juntamente com os grandes benefícios surgem as possíveis violações de segurança e privacidade dos usuários. Esta monografia tem como objetivo principal apresentar um breve histórico do desenvolvimento e funcionamento da tecnologia RFID, abordando com maior profundidade seus aspectos de segurança, ameaças, vulnerabilidades e alguns protocolos de segurança existentes na literatura.

Palavras-chave: RFID, segurança, privacidade, protocolo.

ABSTRACT

Radio-Frequency IDentification (RFID) consists of a wireless data transmission technology through radio signals. RFID technology has been expanding in a number of distinct areas, particularly in industries seeking data automation. However, along with the great benefits arise the possible breaches of security and privacy of users. This monograph aims to present a brief history of the development and operation of RFID technology, addressing more deeply its security aspects, threats, vulnerabilities and some security protocols existing in the literature.

Keywords: RFID, security, privacy, protocol.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

DOS Denial of Service – Ataque de Negação de Serviço

ID Identity – Identidade

IEEE Instituto de Engenheiros Elétricos e Eletrônicos

IFF Identification Friend or Foe - Identificação amigo ou inimigo

KHZ Quilo-Hertz

RFID Radio-Frequency IDentification - Identificação por Radiofrequência

UFPB Universidade Federal da Paraíba

UHF Ultra High Frequency - Freqüência Ultra Alta

SUMÁRIO

1 INTRODUÇÃO

A tecnologia de Identificação por Radiofrequência (RFID) vem ganhando um grande espaço em diversas áreas de pesquisa assim como no ambiente industrial, comercial e até mesmo pessoal. Essa inovação tecnológica se encaixa em todos as áreas que necessitam de automação no processo de reconhecimento dos dados de forma ágil e automática, e com isso possibilitando a identificação de objetos sem a necessidade de contato físico, com o auxílio de sistemas *web* ou até mesmo aplicações mais robustas como a de controle de grandes estoques.

O sistema RFID é basicamente composto por transponder (etiqueta e/ou *tags*) que transmitem informações para o *transceiver*, também conhecidos como leitor de etiqueta. Desta forma, recebe as informações contida nas *tags*, através de uma antena e assim transmitindo os dados para um servidor de banco de dados, e com isso, a informação é captada e decodificada na aplicação. Internamente, as *tags* comportam uma antena para emitir e receber os sinais eletromagnéticos, mais comumente em *Ultra High Frequency (UHF)*, um chip que inclui um modulador e demodulador para o sinal, juntamente com outro circuito para memória, processamento de informações e possivelmente funcionalidades dedicadas a tarefas específicas, como medir a escala de um fenômeno físico (OUAFI, 2012).

Atualmente existem diversos tipos de RFID, entretanto os mais comuns são os ativos e passivos. Want (2006), afirma que as *tags* ativas são aquelas que requerem uma fonte de energia, ou seja, existe a necessidade de ter uma bateria presente no dispositivo para que haja o funcionamento correto, o que leva a gerar mais custos na adoção deste tipo de *tag*. Já as *tags* passivas são interessantes porque não necessitam de baterias ou manutenção. Basicamente a diferença entre os dois tipos anteriormente citados, é a presença de baterias nos ativos de identificação e com isso é possível um maior campo de alcance entre os dispositivos. Ouafi (2012), apresenta as *tags* híbridas, mais conhecida como semi-ativas, que utilizam a bateria apenas para realizar operações internas, entretanto contam com o sinal do leitor para alimentar sua antena e seu modulador.

A tecnologia presente no RFID sem dúvidas é um ponto importante para os dias atuais, principalmente para aquele que busca agilidade em seus processos. Devido ao fato de suas informações serem transmitidas por ondas de radiofrequência, é importante que o contexto aplicado esteja seguro. Caso o sistema esteja desprotegido, leitores clandestinos com o intuito de burlar ou obter informações da *tag* conseguem com uma

maior facilidade esse objetivo, causando assim um potencial risco para a adoção desta tecnologia no contexto organizacional.

No trabalho desenvolvido por Mubarak (2011), ele cita que os problemas de segurança geralmente estão relacionados à escuta clandestina, interceptação de mensagens e ataques a sistemas RFID. Estes tipos de ataques podem ser divididos em ataques ativos e ataques passivos. Ataques ativos, com interceptação humana e ataques de personificação são criados para a negação de serviço para sistemas RFID e normalmente a *tag* será o alvo, enquanto que, escutas e roubo de informações sãos um tipo de ataque passivo.

1.1 Objetivos

1.1.1 Objetivos Gerais

Identificar os aspectos teóricos de segurança em RFID e apresentar métodos existentes na literatura para proteção de ameaças e vulnerabilidades deste tipo de tecnologia.

1.1.2 Objetivos Específicos

São objetivos específicos deste trabalho:

- Realizar uma revisão bibliográfica com o objetivo de apresentar as principais características técnicas de RFID, suas vulnerabilidades e ameaças sofridas em um contexto de sua aplicação em diversas áreas;
- Apresentar algumas soluções existentes na literatura, visando discutir o método mais adequado para proteção de ameaças existentes;

1.2 Justificativa

Atualmente a utilização de RFID vem ganhando seu espaço em meio à outras tecnologias de identificação. Com isso, as ameaças aos usuários que utilizam este tipo de tecnologia vêm se tornando cada vez mais constantes devido às características dos dispositivos ou aplicações que não planejam a segurança das partes envolvidas.

A proposta deste trabalho é identificar quais são os níveis de segurança atualmente existentes no contexto da aplicação do RFID, tendo em vista que a segurança das

informações presentes nos componentes compostos pelo RFID é um assunto que ainda é muito explorado devido às diversas formas de interceptação dos dados.

1.3 Metodologia

Para efetivo desenvolvimento dos objetivos específicos em um corpo de análise e argumentação, adota-se como processo metodológico de caráter exploratório e descritivo, com base em um estudo comparativo entre conteúdos de diferentes autores, em uma revisão bibliográfica que permite abranger uma maior área de conhecimento sobre o assunto em questão, utilizando artigos de pesquisa, revisão, livros e revistas. A busca foi realizada nas bases de dados do IEEE, Google, Google Acadêmico, com as palavras chaves "*security*", "RFID", "*protocol* RFID", em inglês e português.

Para a seleção das fontes, foram consideradas como critério de inclusão as bibliografias que abordassem a segurança e os métodos utilizados para combater as ameaças existentes relacionados a tecnologia RFID e trabalhos publicados entre 2002 a 2018, onde os textos se encontram disponíveis completamente. Partindo dessa lógica, foram excluídas aquelas que não atenderam a temática.

Os resultados quantitativos e qualitativos deste presente trabalho serão acompanhados de análise direcionada ao contexto que se encaixa o objeto de estudo, de forma que consiga cumprir os objetivos propostos, para a realização deste trabalho científico.

1.4 Organização do trabalho

Este trabalho está organizado em quatro capítulos, que são expostos da seguinte forma:

O Capítulo 1 apresenta a definição do problema e as dificuldades que ele pode gerar, os objetivos gerais e específicos, a justificativa e a metodologia.

O Capítulo 2 apresenta a tecnologia RFDI onde se tem uma breve introdução sobre tema abordado, sua evolução histórica e arquitetura.

O Capítulo 3 apresenta os aspectos de segurança da tecnologia em questão, no qual é apresentado suas vulnerabilidades, ameaças e protocolos para proteção dos quesitos de segurança abordado.

O capítulo 4 apresenta as considerações finais do trabalho, incluindo os objetivos atingidos e recomendações para trabalhos futuros sobre o assunto.

2. Identificação por Radiofrequência

2.1 Introdução

A abreviatura RFID vem do termo em inglês *Radio Frequency IDentification* e atualmente é conhecida como Sistema ou Tecnologia de Identificação por Radiofrequência. No decorrer deste trabalho, será utilizado apenas a sigla RFID, por fins de padronização. (MONTALVÃO, 2011)

O RFID utiliza ondas de rádio em diversas faixas de frequência para identificação dos objetos de forma automática. Essa tecnologia pode ser aplicada em contextos que variam de seres humanos, controles de acesso ou até mesmo em veículos. Segundo Sousa (2010), atualmente o RFID vem ganhando espaço entre outras tecnologias como: código de barras, sistemas de identificação biométrica, cartões inteligentes de contato e reconhecimento ótico de caracteres.

2.2 Evolução histórica

Segundo Pedro (2012), as ondas de rádio se tornaram significativas na comunicação, quando Guglielmo Marconi obteve sucesso ao transmitir sinais de rádio que atravessaram o Oceano Atlântico em 1901 e a partir disso foi possível o envio e recepção de informações de diversos formatos.

Em 1935, Robert Alexander Wantson-Watt contribuiu na evolução do radar. Com isso ele fez um experimento que conseguia a localização de objetos fictícios utilizando as ondas de rádio. Na época, a solução proposta por ele foi a mais completa.

Na segunda guerra mundial, os ingleses utilizaram o radar como forma de defesa, tendo em vista que era possível detectar a presença ou não de aviões, entretanto, assim como os alemães e outros envolvidos na guerra, havia o problema de não conseguir identificar quem era aliado ou inimigo. Por consequência, novas ideias foram surgindo diante do problema que estava sendo criado e com isso foi idealizado o sistema IFF (*Identification Friend or Foe*), mais conhecido no Brasil por “amigo ou inimigo”.

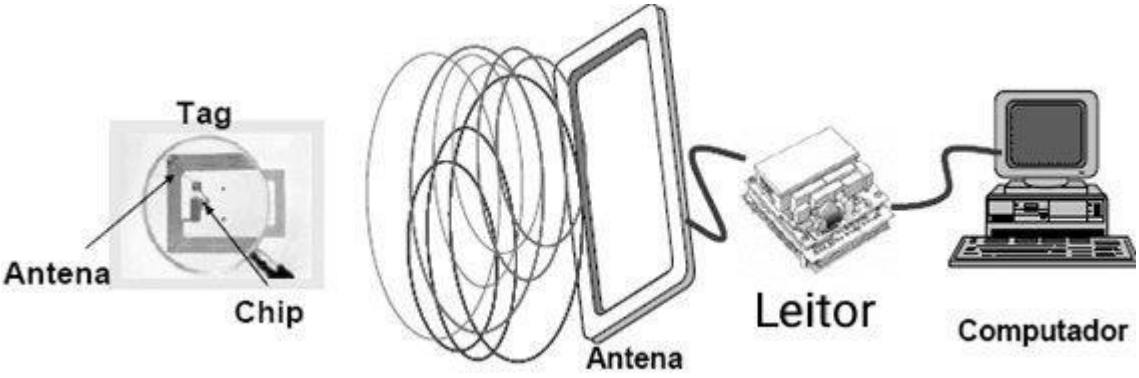
Segundo Pedro (2012), essa solução utilizava um transponder de longo alcance que modulava, de forma ativa, o sinal de resposta ao sinal enviado pelo radar em terra e como consequência, isso permitiu tornar o processo de identificação dos aviões mais simples e rápido. Essa técnica pode ser considerada o primeiro passo para a criação da tecnologia RFID.

2.3 Arquitetura RFID

Em um sistema RFID é necessário basicamente quatro componentes essenciais para o seu bom funcionamento, que são: *tag*, leitor, antenas e um *software* de gerenciamento.

A Figura 1 ilustra o funcionamento básico desses componentes.

Figura 1. Ilustração de um sistema de RFID genérico.



Fonte: PUHLMANN, 2015.

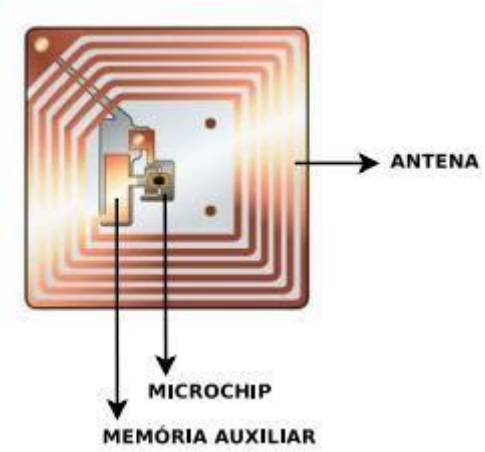
Na Figura 1 é possível ver como funciona a estrutura básica de um sistema RFID com a interação básica entre seus componentes. A *tag* transmite suas informações para um leitor no momento que é detectado algum campo de radiofrequência de sua antena. Após o leitor receber a identificação e os dados da *tag*, estes são transmitidos ao computador que alimentará o banco de dados da aplicação RFID.

2.3.1 *Tags*

O transponder derivado dos termos em inglês *Transmitter-responder* (transmissor e respondedor) (MANISH; SHAHRAM, 2005) ou mais conhecido como *tag*, é um dispositivo que pode armazenar e transmitir dados para um leitor sem a necessidade de

contato, usando ondas de rádio (LAHIRI, 2005). A *tag* tem o objetivo de anexar fisicamente a um objeto, os dados referentes a ele.

Figura 2. Exemplo de uma *Tag* RFID.



Fonte: MOTA, 2015.

A Figura 2 mostra a estrutura básica de uma *tag*, sendo que, no centro da mesma tem um microchip e uma memória auxiliar; e ao redor do chip tem-se a antena de comunicação formada por linhas ao redor de toda *tag* (MOTA, 2006).

As *tags* podem ser classificadas de acordo com a utilização ou não de bateria, sendo assim, conhecidas como *tags* ativas, passivas e semi-passivas. A energia mínima para responder corretamente a leitora varia por cada tipo de *tag* e com isso fica dependente do seu tipo ou padrão pertencente.

De acordo com Klair et al. (2010), as *tags* passivas não possuem fonte de energia e com isso a sua fonte de carga é a partir do sinal do leitor. Já as semi-passivas possuem as características das *tags* passivas, entretanto tem a vantagem de possuir fonte de energia e com isso conseguir alimentar seu microchip quando necessário ou quando não estiver próxima a um leitor. As *tags* ativas, são aquelas que possuem fonte de energia própria e com isso pode estabelecer comunicação por conta própria, porém seu custo é mais alto comparado às demais.

Na figura 3 pode-se identificar a diferença de uma etiqueta ativa e passiva, principalmente em relação ao tamanho da etiqueta ativa que corresponde proporcionalmente aos componentes que nela existem.

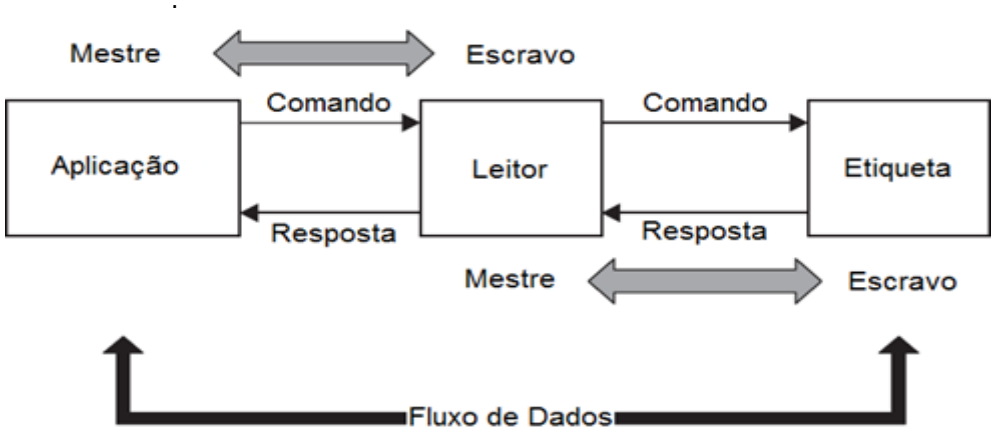
Figura 3. Diferença de tamanho entre a *tag* ativa e a *tag* passiva**.**

Fonte: SMILEY, 2016.

2.3.2 Leitor

O leitor, por sua vez, é o responsável por obter os dados das *tags* e disponibilizá-los em um sistema com interface gráfica ou armazenar em um banco de dados. Alguns leitores de RFID, também possuem o recurso de escrita na *tag*, no qual utilizam do princípio mestre-escravo (FINKENZELLER, 2003), no qual o leitor assume o papel de mestre e a *tag* apenas responde aos comandos dele, que pode ser visto na Figura 4.

Figura 4. Princípio de funcionamento mestre-escravo usado em leitores RFID.



Fonte: Montalvão, 2016.

2.3.3 Antenas

As antenas emitem ondas de radiofrequência para realizar a ativação da *tag* e ler ou escrever dados na mesma. Segundo Godoy Viera (2007), as antenas são utilizadas para irradiar ondas eletromagnéticas que por sua vez, induzem uma corrente nas pequenas antenas das *tags* RFID passivas, fornecendo energia ao microchip para modular um sinal de resposta com as informações contidas nas *tags*.

Estas antenas estarão presentes nas *tags* e também nos leitores, podendo assumir diversos tamanhos e formatos, dependendo de uma série de fatores técnicos, tais como: distância entre leitor e etiqueta, potência de transmissão, frequência de operação etc.

Na Figura 5 é apresentado um tipo de leitor RFID com as antenas possuindo um formato de portal por onde uma grande quantidade de produtos com *tags* podem ser lidos. Esse tipo de leitor é muito utilizado em empresas de logística e produção industrial.

Figura 5. Layout de leitor e antenas no formato de portal.

Fonte: BHATT & GLOVER, 2007.

3. Segurança em RFID

Os sistemas de informações são ambientes que abrangem diversos tipos de informações pessoais. Com isso, é importante que o mesmo tenha garantia de que está cumprindo os três pilares da segurança da informação, que são: confidencialidade, integridade e disponibilidade.

Segundo Engberg (2004), a privacidade do consumidor pode ser ameaçada a partir do momento que o usuário interage com um produto que tenha habilitado o RFID, seja antes da efetivação da compra, assim como no pós-venda de um produto.

Segundo Stallings (2002), um sistema seguro deve cumprir alguns atributos:

- **Privacidade:** É a garantia de que a informação estará protegida de possíveis interceptadores que não sejam autorizados a ter acesso àquela informação. Levando em consideração a comunicação entre a *tag* e o leitor, a privacidade é algo essencial para manter a conexão de forma que os dados do usuário estejam protegidos.
- **Autenticação:** É um fator chave neste processo de transmissão de dados, pois, garante que a informação transmitida foi captada pelo destino correto.
- **Integridade:** Garantia de que o que foi transmitido não foi violado de forma alguma, durante a transmissão.
- **Não repúdio:** elimina a possibilidade de um dos envolvidos (receptor ou remetente) negarem que aquela informação é sua.
- Controle **de acesso:** O controle de acesso é capaz de limitar e controlar o acesso da informação. Utilizando o contexto do RFID, o controle de acesso pode ser interessante na situação em que seja configurado para que apenas os leitores autorizados consigam ler as informações contidas nas *tags*.
- **Disponibilidade:** a disponibilidade consiste em que o sistema esteja disponível sempre para pessoas devidamente autorizadas.

3.1 Vulnerabilidades

A tecnologia RFID apresenta características básicas de armazenamento e leitura de dados em seus componentes. Com isso, a inserção desta tecnologia sem a precaução de atentar aos aspectos de segurança, podem causar problemas graves aos seus usuários. O RFID é comparado com o surgimento da internet. A princípio, a preocupação com a

segurança na internet era algo dispensável, e atualmente, mesmo com a evolução desse serviço, ainda se encontra vulnerável a vírus e ataques adversários (AHSON; ILYAS, 2008).

Atualmente, grandes setores aplicaram o uso do RFID em seu contexto, tendo a finalidade de facilitar seus processos ou até mesmo sendo utilizado para a segmentação da segurança pessoal e patrimonial. Entretanto, existem alguns pontos que acarretará problemas para a empresa ou contexto aplicado, caso a tecnologia seja implantada em grande escala e com a mínima precaução com a segurança. Os exemplos a seguir enfatizam os possíveis problemas causados devido ao uso inadequado da tecnologia RFID.

- **Violação de integridade**: uma etiqueta possuir dados relacionados ao produto ou pessoa em que foi utilizado. No caso em que houver a remoção da etiqueta do contexto original e for aplicado em um contexto genérico, acarretará sérios problemas ao proprietário;
- **Cópia de etiquetas:** uma pessoa com conhecimento técnico sobre a tecnologia RFID, poderá copiar os dados que estão presentes na etiqueta e criar uma nova etiqueta clonada com os dados da etiqueta original;
- **Monitoramento:** obter os dados da etiqueta para uso impróprio sem a necessidade de ter a etiqueta fisicamente.

3.2 Ameaças

A utilização da tecnologia é adotada de acordo com a necessidade, desse modo, seu contexto pode ser aplicado em diversos aspectos como rastreamento de objetos, pessoas ou até mesmo um controle de um grande estoque. A prontidão na qual são feitas as atividades que antes do RFID eram realizadas de forma lenta e falha é muito perceptível, gerando uma maior agilidade nos processos de identificação.

Segundo Filho (2009), os principais ataques relacionados a tecnologia RFID são: *Sniffing*, Rastreamento Clandestino, *Cloning*, Ataque de *Replay*, Negação de Serviço, RFID *exploits* e Vírus. Em seguida, os ataques citados anteriormente serão apresentados resumidamente, de forma que serão expostos os princípios de cada uma dessas ameaças.

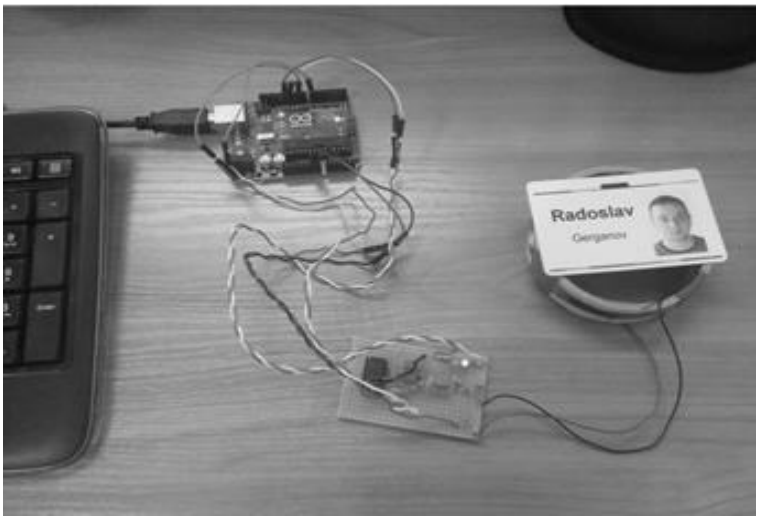
***Sniffing*:** Este tipo de ataque consiste em atacantes que utilizam leitores não autorizados para capturar informações das *tags*. As informações são obtidas através de interceptações das mensagens durante a comunicação entre a *tag* e um leitor autorizado.

Desta forma, esse ataque pode ser um grande problema em relação à privacidade das informações existentes na *tag*. Por exemplo, o atacante pode obter informações pessoais de um veículo que possui rastreamento por meio de RFID e com isso utilizar essas informações para fins não autorizados.

Rastreamento Clandestino: Ao ler as informações recebidas da *tag* RFID, um invasor poderá rastrear a localização e o movimento de um objeto ou pessoa. Quando uma *tag* é anexada a um objeto e o objeto entra no campo do leitor RFID, a leitura RFID pode identificar o objeto e localizar sua posição.

***Cloning*:** Tendo em vista que as *tags* possuem armazenamento para guardar seus códigos, esses ficam vulneráveis a serem copiados, assim como qualquer código fonte. Sendo assim, um atacante que tiver acesso a uma *tag* básica, ou seja, que não possui mecanismo de controle de acesso, o mesmo pode copiar esse código que possui as informações e clonar para uma *tag* clandestina. Na Figura 6, tem-se um leitor de clonagem baseado em Arduino juntamente com um crachá passivo RFID de 125 KHz.

Figura 6. Leitor de clonagem baseado em Arduino.

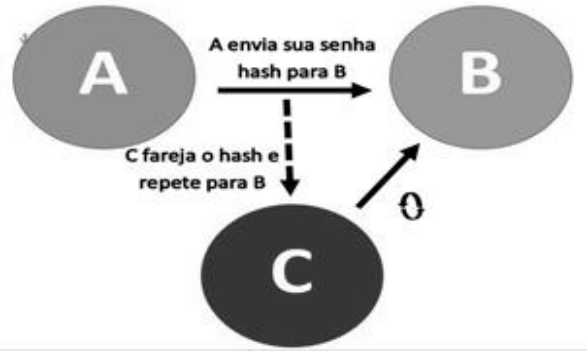


Fonte: Cloning RFID Cards.

Ataque de *Replay*: A característica básica deste tipo de ataque é que atacantes podem interceptar e retransmitir as mensagens RFID, com o objetivo de burlar o sistema que utiliza a tecnologia. Um invasor intercepta a mensagem de comunicação que flui entre o leitor e as *tags* e ele registra a resposta da *tag*, que pode ser usada como resposta à solicitação do leitor.

Na figura 7 é ilustrado um ataque de replay, no qual (A) envia sua senha com hash para (B) com isso (C) intercepta o hash e replica para (B).

Figura 7. Ilustração de um ataque de Replay



Fonte: Autoria própria.

Negação de Serviço: Quando um leitor solicita informações de uma *tag*, ele recebe o ID de identificação e o compara com o ID armazenado no servidor de banco de dados. Tanto o leitor RFID como o servidor *backend* estão vulneráveis a ataques de negação de serviço. Quando o ataque DoS (Denial Of Service, em inglês) ocorre, as *tags* não conseguem verificar sua identidade com o leitor e, como resultado, o serviço é interrompido.

O objetivo da negação de serviço não é roubar ou modificar informações, mas sim desativar o sistema RFID para que o mesmo não seja utilizado. Ao falar sobre ataques DoS em redes sem fio, a primeira preocupação é ataques de camada física, como interferência.

RFID *exploits*: Neste tipo de ataque, é utilizada a tecnologia RFID para explorar vulnerabilidades de segurança existentes no sistema de processamento de dados. Quando um leitor de RFID ler os dados de uma tag, o mesmo espera receber informações em um determinado formato. Porém, uma pessoa mal-intencionada pode escrever dados cuidadosamente criados, cujo formato e conteúdo são tão inesperados que podem corromper o *software* do leitor de RFID e, potencialmente, seu banco de dados também.

Vírus: Como qualquer outro sistema de informação, o RFID também é propenso a ataques de vírus. Na maioria dos casos, o banco de dados é o principal alvo. Um vírus

RFID pode destruir ou divulgar os dados de *tags* armazenados no banco de dados, interrompendo o serviço ou bloqueando a comunicação entre o banco de dados e o leitor.

3.3 Proteção contra ameaças

A segurança da informação que compõe a etiqueta RFID é um fator crítico na motivação do surgimento de novos protocolos de segurança, pois tem-se alguns fatores positivos e negativos sobre esta tecnologia e com isso, para garantir a segurança e integridade dos dados que é transmitido pelas *tags* de RFID é necessário a utilização de métodos adequados para manter a privacidade dos dados e a autenticação segura. Com a percepção das inúmeras falhas de segurança relacionadas à aplicações com a utilização de RFID, surgiram diversas pesquisas com ênfase neste problema.

Diante das ameaças apresentadas, serão mostradas as principais formas de combater os ataques que foram anteriormente citados. Filho (2009) em suas pesquisas, dividiu essas medidas de proteção em três classes: as utilizadas em *tags* básicas, as *tags* que possuem criptografia e através do uso do RFID *Firewall*.

As *tags* básicas não possuem recurso de criptografia nem bons geradores de números pseudo-aleatórios. Por outro lado, *tags* com criptografia possuem algoritmos criptográficos, geralmente criptografia com chaves simétricas, o que permite a implementação de algoritmos de criptografia e mecanismos de autenticação. Tanto as *tags* básicas quanto as com criptografia visam utilizar a menor quantidade possível de recursos de processamento, bateria e memória. O objetivo destas restrições é permitir a produção de *tags* de baixo custo. (FILHO, 2009).

Com o objetivo de combater os ataques sofridos pela tecnologia RFID, surgiram métodos para que a privacidade e segurança dos dispositivos fossem mantidas. Abaixo, são apresentadas algumas medidas que podem ser tomadas para combater as ameaças existentes.

Killing: A abordagem mais simples para a proteção da privacidade do consumidor é "matar" as *tags* RFID. Por exemplo, em uma situação em que um consumidor escolhe um determinado produto em um supermercado, ele se dirige ao caixa e com isso o operador envia o comando *kill* para a *tag* que compõe o produto que está sendo adquirido, fazendo com que a *tag* perca sua funcionalidade. Com isso, a *tag* fica permanentemente desativada. O comando *kill*, está disponível em apenas alguns tipos de etiquetas e é

protegida por um PIN, que tem a finalidade de impedir a destruição por leitores não autorizados (JUELS, 2006).

A desativação da *tag* através do comando *kill* é uma medida de privacidade altamente eficaz, entretanto, esse método descarta todos os benefícios que a tecnologia RFID poderia fornecer ao consumidor após efetuar a compra de um produto que utilizava uma etiqueta de identificação. Em casos como, o aluguel de mercadorias e bibliotecas, a *tag* não pode ser desativada, pois como os objetos que esses cenários oferecem muita das vezes são retornáveis, as *tags* precisam estar ativas para que assim possam ser identificados os itens novamente.

Gaiola de Faraday: Este método utiliza o princípio da utilização de uma malha de metal que é impenetrável para as ondas de rádio que são enviadas ou recebidas, com a finalidade de impedir a comunicação com os dispositivos de RFID (JUELS et al, 2003). Desta forma, os usuários podem hoje comprar Gaiolas de Faraday na forma de carteiras e capas para proteger seus dispositivos RFID contra leitores não autorizados.

***Hash Lock*:** O método de criptografia *Hash Lock*, foi projetado para caber nas etiquetas que tem pouca memória (WEIS, 2003). Segundo Mota (2006), o controle de acesso através deste método, consiste em um mecanismo básico baseado nas funções *hash*, no qual é necessário que as *tags* tenham uma função *hash* otimizada em seu *hardware*. As Tabelas 1 e 2 apresentam o funcionamento básico deste procedimento.

Quadro 1. Procedimentos para o travamento da TAG com o método *Hash Lock*.

TRAVAMENTO DA TAG
1. O leitor X seleciona uma chave aleatória *key e* calcula *metaID = hash(key);* 2. O leitor X escreve a *metaID na tag;* 3. A tag entra no estado “travado”; 4. O leitor X armazena no banco de dados o par(*metaID, key)* localmente;

Fonte: Autoria própria.

Quadro 2. Procedimentos para o destravamento da TAG com o método *Hash Lock*.

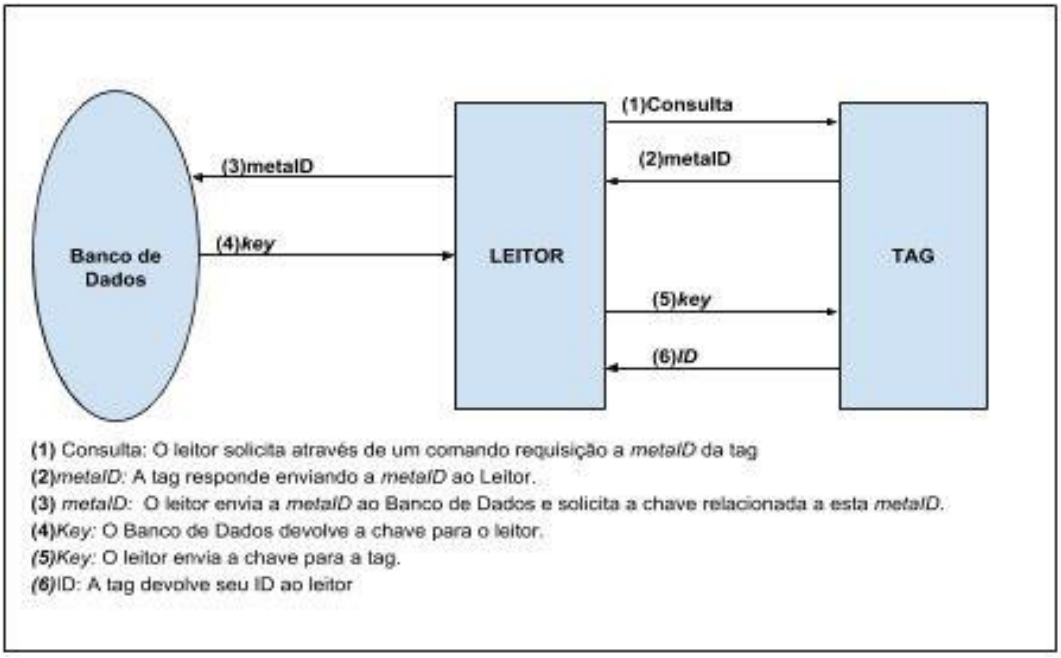
DESTRAVAMENTO DA TAG
1. O leitor X solicita a *metaID* da tag; 2. O leitor X procura o par(*metaID e key)* localmente; 3. O leitor X envia a chave *key para a tag;* 4. A tag confere se (hash(key)=*metaID)* e destrava caso positivo.

Fonte: Autoria própria.

Com isso, somente leitores previamente autorizados podem destravar as *tags* para a realização de consultas, pois leitores clandestinos não possuem o par (metaID, key) e com isso é realizado a proteção contra leitores não autorizados.

Essa solução está aprimorando cada vez mais a segurança e privacidade das *tags* RFID, entretanto, esse protocolo possui uma desvantagem no qual um valor *hash* que esteja de forma estática, ainda possa ser rastreado. A Figura 8 ilustra o algoritmo.

Figura 8. Ilustração do método *Hash Lock*.

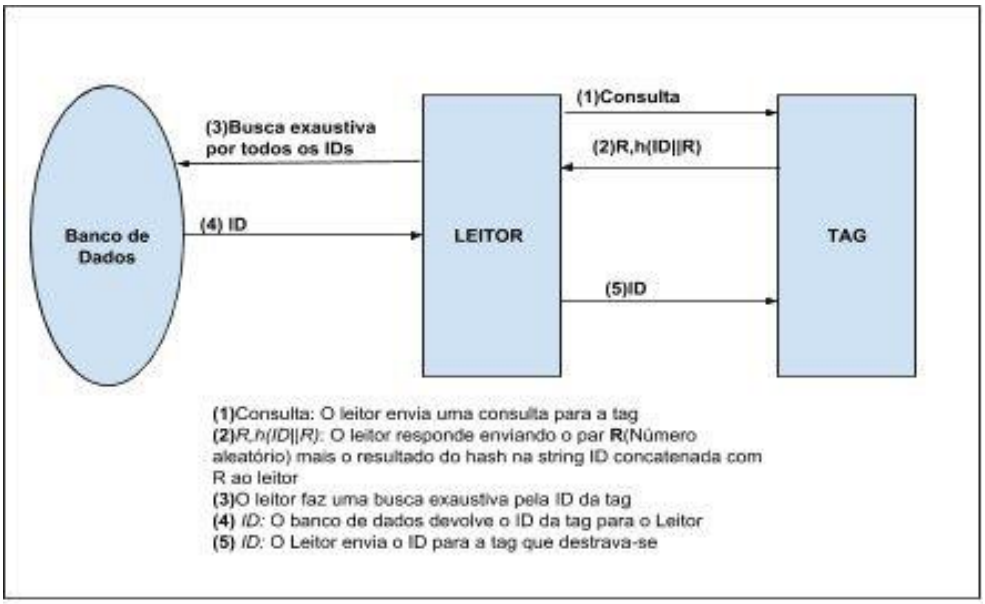


Fonte: Adaptado de MOTA, 2006.

***Randomized Hash Lock*:** Esse protocolo possui as mesmas características da solução anterior, porém utiliza uma função que gera números aleatórios, no qual são adicionados e com isso evita que a *tag* seja rastreada (WEIS, 2003). O gerador de números

aleatórios adiciona uma combinação que permite uma variação no momento da transmissão da identificação única da *tag*. De acordo com que for sendo encontrada alguma correspondência, o leitor poderá desbloquear a *tag* enviando o valor do ID. Os IDs aleatórios são força bruta verificada no banco de dados que armazena todos os números aleatórios (SPRUIT; WESTER, 2003). A Figura 9 ilustra o algoritmo.

Figura 9. Ilustração do método Randomized Hash Lock.

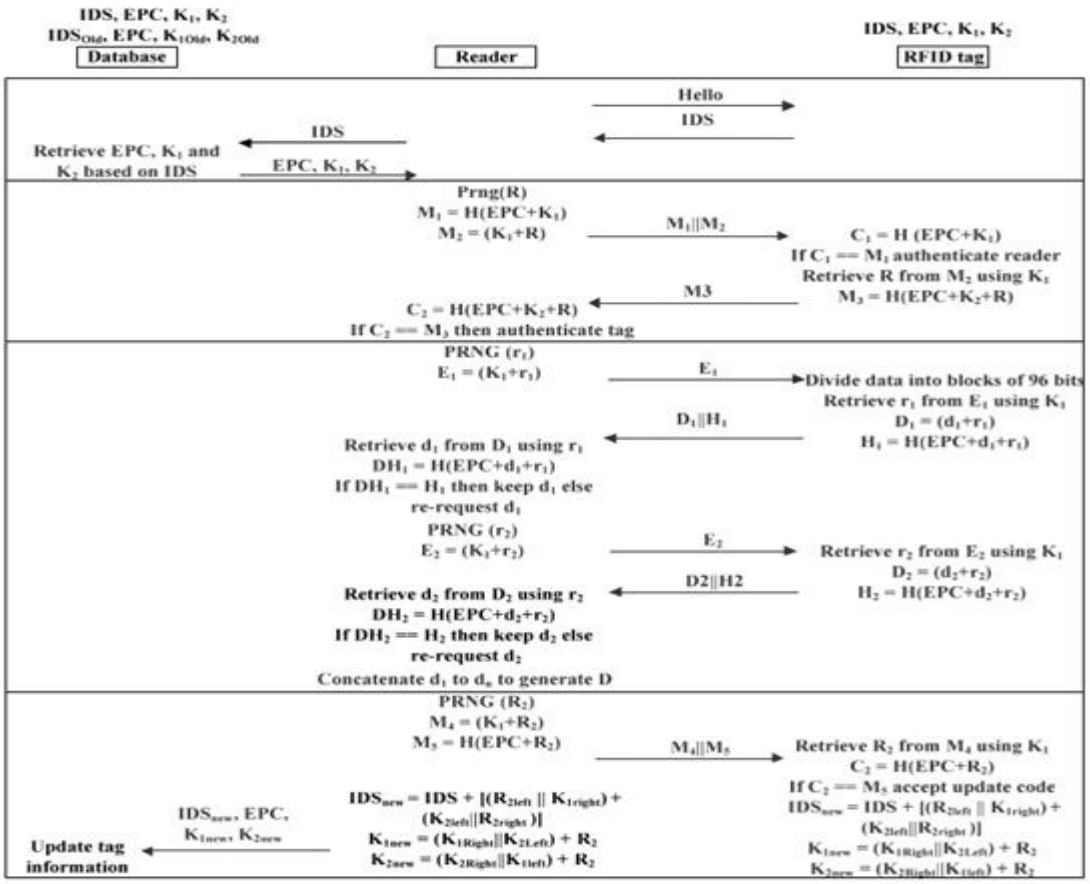


Fonte: Adaptado de MOTA, 2006.

Fernando e Abawajy (2011) desenvolveram um protocolo de segurança no qual permite autenticação mútua entre o leitor e a *tag*, assim como a comunicação de forma segura dos dados da *tag*. O protocolo apresentado utiliza um método híbrido para fornecer um alto nível de segurança. Para isso, é empregado 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 considerado resistente a um grande número de ataques comuns como pôr exemplo o ataque de replay.

Figura 10. Protocolo de Autenticação mútua proposto pelos autores Fernando e Abawajy (2011).

H (x) - função hash unidirecional na entrada x
PRNG (x) - Geração de PRNG x 96 bits
X + Y - Função XOR em X e Y
X || Y - Concatenação de X e Y
X == Y - operação de comparação em X e Y



Fonte: FERNANDO E ABAWAJY, 2011.

Malek e Miri (2012) também desenvolveram 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* armazenem matrizes esparsas, conforme o protocolo McEliece. Operações computacionais complexas são substituídas 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, tem-se que o protocolo proposto assegura que apenas leitores autorizados possam consultas as *tags*, protegendo assim o sistema contra violação de privacidade. Na Figura 12 é demonstrado o funcionamento do protocolo proposto, no qual a etiqueta RFID é representada por T e o leitor por R.

Figura 11. Protocolo proposto por Malek e Miri (2012) utilizando a autenticação mútua.

Algorithm 1 Mutual authentication of RFID tags and readers

1.	R:	$\{ID - REQ\} \longrightarrow T$
	T:	find $\{rF_1 \oplus a_{\text{id}}F_2, a_{\text{id}}\}$ for R, o.w. quit
	T:	pick e randomly s.t. $w(e) = \frac{d-1}{2}$
	T:	send $y = rF_1 \oplus a_{\text{id}}F_2 \oplus e \longrightarrow R$
5.	R:	decrypt y to find r, a_{id} and e
	R:	verify T if r received is correct for a_{id}
	R:	pick a random $t \in \mathbb{F}_{2^N}$
	R:	set $d_0 = rF_1 \oplus a_{\text{id}}F_2 \oplus t$ and $d_1 = a_{\text{id}} \oplus h(eA_t)$
	R:	$S = \{d_0, d_1\} \longrightarrow T$
10.	T:	compute $d_0 \oplus rF_1 \oplus a_{\text{id}}F_2$ to find t
	T:	using t and e calculate eA_t
	T:	check if $(d_1 \oplus h(eA_t)) = a_{\text{id}}$, o.w. refuse R
	T:	send $OK \longrightarrow R$
	R:	pick a random $r' \in \mathbb{F}_{2^{k_1}}$
15.	R:	send $y' = r'F_1 \oplus a_{\text{id}}F_2 \oplus e \longrightarrow T$
	T:	replace $\{rF_1 \oplus a_{\text{id}}F_2, a_{\text{id}}\}$ with $\{y' \oplus e, a_{\text{id}}\}$

Fonte: MALEK E MIRI, 2012.

Juels (2006), propôs uma solução na qual se utiliza um conjunto de chaves de criptografia onde o leitor/*tag* tem um conjunto de chaves simétricas. Na solução apresentada, a *tag* classifica aleatoriamente uma chave e envia o seu identificador criptografado para o leitor e com isso, o leitor ao captar a mensagem, realiza uma pesquisa em sua base de dados tendo o objetivo de encontrar uma chave que na descriptografia consiga um identificador válido. Caso encontre, o leitor obtém a chave de criptografia da *tag*.

3.4 Eficácia dos métodos de proteção

Segundo Fernando e Abawajy (2011), o desenvolvimento de protocolos de segurança para sistemas RFID tem como características dois principais desafios, um desses desafios é desenvolver protocolos que possam suportar a grande diversidade de funcionalidades de segurança que são exigidos pelos sistemas RFID em rede e o outro desafio é assegurar que as limitações computacionais sejam poucas o suficiente para que consiga ser implementado em *tags* RFID de baixo custo.

No método de criptografia com chaves simétricas tem-se a garantia da confidencialidade e integridade dos dados de forma que, se um usuário X utiliza uma determinada chave juntamente com um algoritmo de codificação para criptografar a mensagem, enquanto o usuário Y utiliza a mesma chave e um algoritmo de decodificação igual para decodificar a mensagem, se houver correlação entre ambas o algoritmo irá a operação de decodificação da mensagem e com isso o usuário Y poderá ter acesso a mensagem. Entretanto, cada par de usuários tem que obter sincronia a uma única chave e com isso se mais usuários quiserem manter a comunicação utilizando esse método serão necessários x (x - 1) /2 chaves simétricas, acarretando problemas de armazenamento e distribuição de chaves.

As funções *hash* ainda são grandes e poderosas ferramentas de criptografia, no qual se torna bastante eficiente para soluções que necessitam de uma implementação de *hardware* para RFID de baixo custo. Nos protocolos de *hash-lock* citados no capítulo anterior, foram apresentadas algumas características de segurança providas pelo mesmo. No entanto, os protocolos propostos não são privados nem seguros contra bisbilhoteiros desde que o atacante possa rastrear a metaID e representar a *tag* para um leitor legítimo.

A autenticação mútua é um método importante para manter os requisitos de autenticação existentes nos elementos que compõe um sistema RFID. Neste caso, a autenticação mútua pode ser feita entre a *tag* e o leitor, o leitor e o servidor *back-end* e a *tag* e o servidor *back-end*. Nos protocolos de autenticação mútua propostos, são apresentadas suas características para manter a confidencialidade e integridade dos dados através da autenticação entre a *tag* e o leitor.

No protocolo de autenticação mútua proposto, Fernando e Abawajy (2011) afirmam que a confidencialidade dos dados é ocorrida devido a todas as mensagens públicas serem divididas utilizando um algoritmo de *hash* unidirecional ou composto por operações bit a bit, empregando assim um número aleatório (R1, R2, r1, r2,…,rn) ou

operações bit a bit no qual é designado uma chave secreta que é reconhecida apenas pela própria *tag* e leitores autorizados e com isso é quase impossível captar os dados transmitidos. Além desses fatores anteriormente citados, como os números aleatórios mudam após cada bloco de dados e as chaves são atualizadas após cada sessão, o ataque de força bruta terá que ser efetuado diversas vezes para que assim o atacante possa obter qualquer dado importante.

A integridade neste protocolo é possível devido ao fator que sempre que uma mensagem de dados é transmitida, é realizado o envio de outra mensagem de resposta contendo uma *hash*, o que faz com que essa mensagem *hash* possa garantir ao protocolo a integridade dos dados recebidos. O número aleatório recuperado pela *tag* não é o mesmo que o número que o leitor gerou e transmitiu.

Segundo Fernando e Abawajy (2011), a proteção contra *Replay Attacks* pode ser realizada de diversas maneiras no qual uma delas é o atacante tentar armazenar os IDs transmitidos pela *tag* ou a mensagem transmitida pelo leitor e reproduzi-los. Entretanto, no protocolo proposto os IDs são atualizados usando números aleatórios após cada sessão e com isso impedindo o objetivo dos atacantes.

Também é garantida a proteção contra o *Man-in-the-middle* em razão do fato de possuir uma forte autenticação mútua, transmissão confidencial e integridade de transmissão devido ao fato que qualquer alteração será constatada nas verificações de integridade ou então será realizada a mudança dos números aleatoriamente, de forma a fazer com que o atacante e a *tag* tenham números aleatórios diferentes, tornando impossível para o atacante “decriptografar” as mensagens. E como o invasor não consegue acessar até mesmo os números aleatórios usados, ele não poderá descriptografar as mensagens normais que passam por ele.

4. CONSIDERAÇÕES FINAIS

Neste trabalho, foram apresentados os principais aspectos de privacidade e segurança da informação em sistemas RFID, buscando analisar através dos principais conceitos de segurança da informação, quais os níveis de segurança atualmente existentes nos componentes que constituem um sistema RFID.

Para alcançar o objetivo principal da pesquisa, foi realizado uma revisão bibliográfica, apresentando conceitos e alguns modelos de protocolos de segurança existentes. Também foram analisadas as principais vulnerabilidades e ameaças presentes em sistemas que utilizam a identificação por radiofrequência, listando os casos mais comuns e citando quais são os efeitos negativos da falta de planejamento de segurança em aplicações que utilizam a tecnologia RFID.

Desta forma, a pesquisa mostrou que prover a segurança em sistemas RFID é um dos maiores desafios desta tecnologia. Entretanto dos protocolos analisados, o protocolo de autenticação mútua foi o que apresentou mais confiabilidade em sua aplicação, uma vez que foi provado a sua eficiência para atingir os principais níveis da segurança da informação.

Recomenda-se para novas pesquisas, a aplicação de um protocolo de segurança em um contexto atual, bem como a utilização dos pilares de segurança da informação, com o objetivo de provar na prática os protocolos existentes na literatura sobre segurança RFID.

REFERÊNCIAS BIBLIOGRÁFICAS

AHSON, S.; ILYAS, M. **RFID handbook: applications, security, and privacy.** United States of America: CRC Press, 2008.

CLONING RFID CARDS. Disponível em: <http://xakcop.com/post/cloning-rfid/>. Acesso em: 07 de Nov. de 2018.

ENGBERGE, S., HARNING, M.; DAMSGAARD-JENSEN, C. **Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience.** In Conference on Privacy, Security and Trust – PST, New Brunswick. Canadá, 2004.

FERNANDO, H.; ABAWAJY, J. **Mutual authentication protocol for networked RFID**
systems. 2011.

FILHO, J.M.F. **Implementação e Análise de Desempenho dos Protocolos de Criptografia Neural e Diffie-Hellman em Sistemas RFID Utilizando uma Plataforma Embarcada.** Dissertação (Mestrado em Ciências) - Universidade Federal do Rio Grande do Norte. Natal, 2009.

FINKENZELLER, K. **RFID Handbook: Fundamentals and Applications inContactless Smart Cards and Identification.** John Wiley & Sons, 2ª ed., 2003.

GLOVER, B.; BHATT, H. **Fundamentos de RFID.** Rio de Janeiro: Alta Books, 2007.

HADDAD, C.R.; RIRZZOTTO, F.H.; URIONA, M. **Revisão Estruturada da Literatura sobre RFID e suas Aplicações na Cadeia de Suprimentos.** Revista Espacios.V. 37, nº 08, p-19. 2016.

JENG, A., CHANG, L.C.; CHEN, S.H. **A Low Cost Key Agreement Protocol Based on Binary Tree for EPC global Class 1 Generation 2 RFID Protocol.** IEICE Transactions, 2008.

JUELS, A. **RFID Security and Privacy: A Research Survey.** IEEE Journal On Selected Areas In Communication. V.24, n.02, 2006.

JUELS, A.; RIVEST, R.; SZYDLO, M. **The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy.** Proceedings of the 8th ACM Conference on Computer and Communications Security, ACM Press, 2003.

KLAIR et al. D.K; CHIN, K.K; RAAD, R. **A Survey and Tutorial of RFID: Anti-Collision Protocols.** Communications Surveys Tutorials, IEEE, 2010, 12(3):400–421.

LAHIRI, S. **RFID sourcebook. Indianopolis: Pearson Education.** IBM Press, 2005.

LEI, H.; YONG, G.; NA-NA, L.; ZENG-YOU, C. **A Security-provable Authentication and Key Agreement Protocol in RFID System.** IEEE, 2007.

MALEK, B.; MIRI, A. **Lightweight mutual RFID authentication.** IEE Internacional Conference on Communications. Canadá, 2012.

MANISH, B.; SHAHRAM, M. **RFID Field Guide: Deploying Radio Frequency Identification Systems.** Prentice Hall, 2005.

McELIECE, R.J. **A public-key cryptosystem based on algebraic coding theory.** 42(44):114–116, 1978.

MONTALVÃO, A.C.P.S. **Estudo da conversão de polarização linear-circular em antenas dual-band para leitores RFID portáteis usando metasuperfícies miniaturizadas.** Tese (Doutorado em Engenharia Elétrica e Computação) - Universidade Federal do Rio Grande do Norte. Natal, 2016.

MOTA, R.P.B. **Mecanismos para a melhoria do desempenho de sistemas RFID passivos.** Tese de Doutorado, USP- São Paulo, 2015.

MOTA, R.P.B. **Extensões ao protocolo de comunicação EPC Global para tags Classe 1 utilizando autenticação com criptografia de baixo custo para segurança em identificação por radiofreqüência.** Dissertação (Mestrado em ciência da computação) – Universidade Federal de São Carlos. São Carlos, 2006.

OUAFI, K. **Security and Pvivacy in RFID Sistems.** Tese de Doutorado - École Politechinique Federal de Lausanne. Suiça, 2012.

PEDRO, I.S.G. **Estudo do potencial de aplicabilidade da tecnologia RFID em meio hospitalar.** Dissertação (Mestrado em Engenharia Elétrica e de Computadores- Universidade da Beira Interior. Covilhã, 2012.

PUHLMANN, H.F.W. **Introdução à tecnologia de identificação RFID.** 2015. Disponível em: <https://www.embarcados.com.br/introducao-a-rfid/>. Acesso em: 10 de outubro de 2018.

SMILEY, S. **Active RFID vs. Passive RFID: What's the Difference?.** Disponível em : <https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid>. 2016. Acesso em: 1 de outubro de 2018.

SPRUIT, M.; WESTER, W. **RFID security and privacy: threats and countermeasures.** Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands, 2013.

STALLINGS, W. **Network security essentials.** 2a ed. SP: Prentice Hall, 2002.

VIERA, A.F.G.; VIERA, S.D.G; VIERA, L.E.G. **Tecnologia de identificação por radiofreqüência: fundamentos e aplicações em automação de bibliotecas.** Revista eletrônica de biblioteconomia e ciência da informação. Florianópolis.V. 12, n. 24, p. 182-202, 2007.

WANT, R**. An introduction to RFID technology.** Pervasive Computing, IEEE, 5(1):25–33, 2006.

WEIS, S. A. **Security and Privacy in Radio-Frequency Identification Devices.** Massachusetts Institute of Technology, 2003.