Segurança e Gerenciamento da Rede IoT

J.R. Emiliano Leite, Paulo S. Martins e Edson L. Ursini
School of Technology, University of Campinas (UNICAMP), Limeira-SP,Brazil,
E-mails: j750465@dac.unicamp.br,{paulo,ursini}@ft.unicamp.br

Abstract— The Internet established itself as a network and an international communication tool, enabling the communication of people and computers. The decrease in cost and size of Internet access components let ordinary devices (e.g. TV sets, refrigerators, cookers, air-conditioning systems, residential alarms, and lamps) to access a broader network. More recently, the Internet of Things (IoT) has appeared allowing the increment of intelligence in the various sectors of the economy. The growing application of the IoT needs to be properly understood due to its potential to increase and exploit real-time data and the wealth of information currently available from sensors and RFID. Within this context, this paper presents an overview of this new network environment in terms of its security and management.

Keywords—Mobile Ad-Hoc Networks (MANET*), Wireless Sensor Networks* (WSN), IoT, RFID, NFC, OSI, Bluetooth, Wi-Fi, ZigBee, Security, Management, SNMP.

I. INTRODUÇÃO

A INTERNET consagrou-se como sendo uma "Rede de Redes" e uma ferramenta de comunicação globalizada, inicialmente possibilitando a ligação entre pessoas e entre pessoas e computadores (máquinas). Foi criada nos anos 60 com o objetivo de interligar os ambientes acadêmicos e de pesquisas; com seu crescimento, a Internet foi expandida para a área comercial, aumentando ainda mais o seu uso com o surgimento da forma de busca *WEB (WWW)* e das redes sociais. Atualmente, é impossível imaginarmos nossa vida, sem o uso da Internet, das redes sociais e comerciais.

O conceito de Internet das Coisas (IoT) foi introduzido por Kelvin Ashton em 1999 como resultado de pesquisa de etiquetas eletrônicas RFID na cadeia de produção. Adicionalmente, a utilização de sensores e atuadores foi introduzida, apesar de suas restrições de energia, processamento e memória. Com o avanço da microeletrônica, os preços das interfaces de redes diminuíram, e seu tamanho físico também, viabilizando a introdução de telecomunicações nesses objetos, tornando-os assim "Objetos Inteligentes e Conectados". Dessa maneira, a INTERNET globalizada passou a incorporar os objetos inteligentes, surgindo assim a Internet das Coisas.

Essa nova forma de utilização da Internet visa interligar aparelhos de uso cotidiano, executando assim uma comunicação entre coisas/objetos/aparelhos, possibilitando uma maior automatização do nosso dia-a-dia, por meio do aparelho celular. Possibilita também o incremento de inteligência em diversos setores da economia: *SMART Grid* (Setor Elétrico), *City*, *Building*, *Home*, Logística, Indústria, Hospital, Saúde e Automatização Comercial (Atacado e Varejo), dentre outros. A inteligência e a automação são decorrentes dos acréscimos de processamento, memória e comunicação nos objetos envolvidos. A IoT realiza uma nova transformação digital, conectando dispositivos, incrementando valores de negócios, redefinindo organizações e gerando enorme quantidade de oportunidades. Sem dúvida, esta é uma nova ONDA TECNOLÓGICA que cria uma nova fronteira do mundo conectado com as pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais conectados e capazes de interagirem entre si.

Órgãos internacionais especificaram a padronização internacional aberta, visando a interconexão de objetos e sistemas heterogêneos, de qualquer tipo, modelo e fabricante: IoT-A (Padronização IoT), EPCglobal (Padronização RFID), ITU-T (Telecomunicações), IPSO (Padronização de Objetos Inteligentes), IEEE, 3GPP (Telefones Móveis), IEC/ISO e IETF (Padronização INTERNET). A IoT possui vasto conhecimento documentado em livros e padrões internacionais [1]. Mantivemos a nomenclatura inglesa para ficar compatível com as normas internacionais.

A Pilha de Protocolos IoT foi criada seguindo o Modelo OSI (*Open Systems Interconnection*) da ISO de 7 camadas. A Comunicação é dividida em 7 Camadas devido à complexidade da ligação. O foco da IoT está na Informação transportada (DATA), gerada pelos RFIDs e Sensores. As demais camadas (*Physical*, *link*, *Network&ID*, *End to End*) importam funcionalidades semelhantes àquelas preconizadas no ISO/OSI *Stack*. Os dispositivos conectados são em grande volume, gerando enorme quantidade de dados, apesar do eventual baixo volume de dados gerado individualmente por sensor e RFID.

O Modelo de Referência IoT é composto dos seguintes submodelos, com níveis diferentes de abstrações:

- *Domain*: responsável pela identificação e agrupamento dos sistemas;
- *Information*: responsável pelo transporte das informações geradas pelos Sensores e RFIDs;
- *Functional*: responsável pelo agrupamento das funções existentes nos sistemas;
- *Communication*: responsável pela quebra da comunicação em 7 camadas de protocolos, seguindo o Modelo OSI da ISO.
- *Trust, Security and Privacy Model*: agrupa funcionalidades de Segurança da Informação, Privacidade e Certificação;
- *Network Management*;

A Figura 1 mostra o Modelo de Referência IoT conforme o entendimento de Telecomunicações do ITU-T [1], ISO e IEC. Como todos os modelos de referência da ITU-T, possui 2 colunas referentes a Gerenciamento de Rede e Segurança, colunas essas que têm funcionalidades espalhadas em todas as camadas do modelo.

.

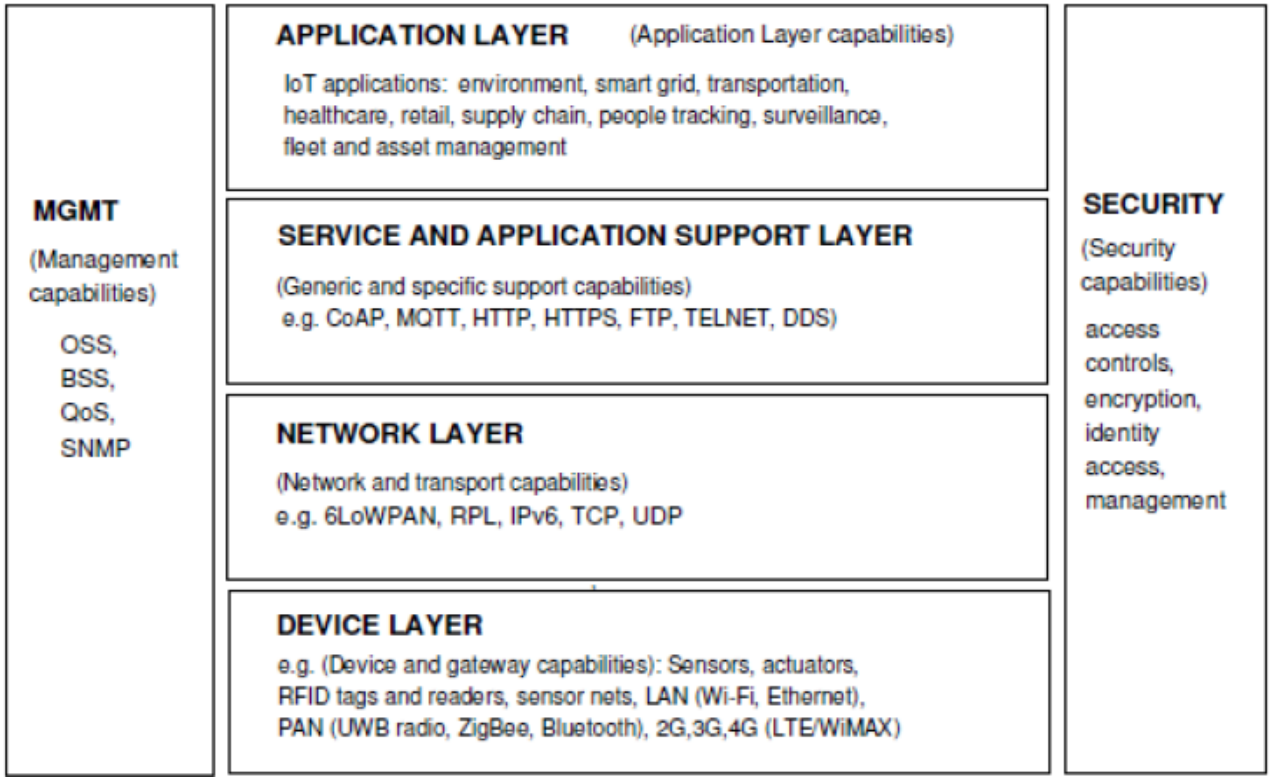

Figura 1 : Modelo de Referência IoT com seus principais protocolos (ITU-T, ISO e IEC)

.

As aplicações estão divididas em diversas Áreas da Economia Mundial: Industrial, Automação Residencial, Transportes, Logística, Hospitalar, Comercial, Energia Elétrica, Cidades Inteligentes, etc. A Tecnologia Celular 5G (D2D) será acrescentada em breve na camada de dispositivos, pois já está em testes pilotos mundiais; com isso, o celular será incrementado com a alternativa da funcionalidade AdHoc. As Tecnologias de Acesso são mostradas na Tabela 1.

O restante deste artigo está organizado com as seguintes secções: Secção II apresenta os trabalhos relacionados. A Secção III mostra a Segurança da Informação na IoT. A Secção IV mostra o Gerenciamento de Rede IoT e finalmente, a Secção V mostra as conclusões.

II. TRABALHOS RELACIONADOS

O artigo de Grabovica et al[2]. apresenta os Mecanismos de Segurança para Redes IoT usuárias de Tecnologias ZigBee, Bluetooth, RFID e WiFi. São mecanismos já existentes nos protocolos atuais e que podem ser utilizados para dar uma melhor segurança na comunicação. O Assunto SEGURANÇA da Informação está no Estado da Arte de IoT.

O artigo de Gonçalves et al[3]. apresenta uma Arquitetura de Segurança para Aplicações de Mobile E-Health no Controle de Medicamentos. Comenta que por motivos de segurança, a Tecnologia RFID é a melhor a ser utilizada na Área Médica; serve para Identificação de Remédios, Equipamentos e Profissionais (Médico, Enfermeiro, Cuidadora, Farmacêutico), garantindo uma Identificação ÚNICA e SEGURA, usando 96 bits de Identificação. Propõe uso de Mecanismos de Segurança nos Protocolos TCP/IP/HTTPS/IPSec. Comenta também sobre a Utilização de LogIN/Senha nos Aplicativos, garantindo a Identidade do Usuário. Comenta a necessidade de se utilizar arquivos LOG contendo todas as intervenções ocorridas com o Paciente. Propõe também a utilização de Protocolos de Segurança mais sofisticados e complexos, com o uso de Chaves Públicas e Privadas, Algoritmos HASH, Criptografias Simétricas e Assimétricas. É um assunto de alta complexidade que proporcionará muitas novas pesquisas.

O artigo de Sallabi et al [5]. apresenta uma Proposta de Arquitetura para Sistemas de Gerenciamento de Redes IoT, baseada no Modelo TMN (Rede de Gerenciamento de Telecomunicações) da ITU (União Internacional de Telecomunicações), comentando que a área de Gerenciamento de Redes IoT está pouco pesquisada, devendo aparecer ainda muitos trabalhos de pesquisas. Apresenta também um Estudo de Caso para SMART

Healthcare, aplicável a Pacientes nos contextos de Residência (Fixo), Escritório (Móvel) e Viagem. Cada um desses contextos exige requisitos de comunicações diferentes. Comenta que as Empresas de Plano de Saúde serão as grandes interessadas em oferecer esse novo tipo de serviço que objetiva retirar pacientes mais cedo do hospital, contratando Empresas de Telecomunicações ISP e Cuidadoras de Pacientes (Novo Modelo de Negócio). Comenta na utilização do Protocolo SNMP (*Simple Network Management Protocol*) [4] como base para a Comunicação de Gerenciamento. O Assunto Gerenciamento de Rede IoT está no Estado da Arte, e é um boa área de pesquisa.

O artigo de Samaniego et al [6]. apresenta o Gerenciamento de Recursos Heterogêneos da IoT, onde se obtém os dados. Esses recursos normalmente são limitados e trabalham com soluções de protocolos proprietários. Cada vendedor oferece sua própria comunicação proprietária visando compatibilidade, eficiência e segurança na comunicação do ambiente restrito até o ambiente de núvem. A necessidade de padrões tem influenciado que usuários exijam implementações de interconexão de coisas heterogêneas seguindo os padrões de gerenciamento ITU-T M.3400. Este artigo apresenta a criação de Recursos Virtuais rodando em Dispositivos de Computação EDGE na núvem, adotando o Protocolo CoAP (Constrained Application Protocol : RFC 7252) na comunicação do Recurso Virtual com estado (usando CoAP REST para buscar os estados) ou sem estado(usando CoAP OBSERVE para receber as atualizações) e a Linguagem de Programação GO para construí-los. A Arquitetura foi desenvolvida em 3 Camadas : View Abstraction Layer (VAL), Hardware Abstraction Layer (HAL) e Physical Layer (PL : Sensores). Foi utilizada Emulação de Clientes para análise experimental.

O artigo de Llia Sotnikov [7] apresenta um Programa de Gerenciamento de Risco em Segurança da Informação. Mostra o framework de segurança NIST Cyber Security envolvendo as seguintes atividades : *Identity, Protect, Detect, Respond and Recover*. Cada uma dessas atividades possui um conjunto de funcionalidades responsáveis em garantir a segurança

O Livro de Gerenciamento de Rede [4] apresenta os principios Básicos do Protocolo SNMP.

Todavia, em nenhum desses trabalhos é apresentada uma visão geral e sumarizada sobre Segurança e Gerenciamento de Rede IoT.

III. SEGURANÇA DA REDE IoT

A IoT selecionou diversas tecnologias padronizadas e utilizadas internacionalmente. Assim sendo, muito dos novos ambientes IoT são parecidos com os atuais existentes na INTERNET Residencial e Empresarial. A maioria das tecnologias é por rádio e sem fio (*Radio Access Technologies*), ou seja, utilizando os padrões IEEE 802.11, IEEE 802.15 e IEEE 802.16, por questões de flexibilidade e alcance.

Tabela 1 : Comparação das Tecnologias de Acesso

TECHNOLOGY	***STANDARD***	***RATE/Frequency***	***POWER***	***RANGE***	***BATTERY***	***TOPOLOGY***	***#NODES***
NFC	ISO/IEC 18092	424 kbps	-	1-10 cm	Months/Years	1 + 1	2
RFID	ISO/IEC 18000	125Khz, 13,56Mhz 800Mhz a 960Mhz 2,45Ghz ou 5,8Ghz	-	metros	-	STAR	Diversos
BLUETOOTH	IEEE 802.15.1	1 Mbps	49mA/0,2mA	1-10 m	Days	STAR	7
ZIGBEE	IEEE 802.15.4	20 to 250 kbps	30mA/356uA	100+m	Months/Years	P2P/STAR	254 A 64516
WI-FI	IEEE 802.11b	54 Mbps	400/20 mA	1-100m	Hours	STAR	64+190cabeadas

O núcleo da IoT é formado por plataformas especializadas em serviços de coleta de dados de dispositivos IoT, processamento de dados e conexão com outros serviços para tomada de decisão em atividades futuras, tais como ativação de atuadores, etc. A maioria das redes IoT utiliza tecnologia sem fio por questões de flexibilidade, sendo assim mais susceptível a ataques gerais de redes sem fio, tais como: DoS (*denial of service*), MITM (*man-in-the midle*), ESCUTA (*eavesdropping*), modificação de mensagem e apropriação de recurso. Adicionalmente, cada tecnologia possui também outros pontos vulneráveis que devem ser considerados na fase de projeto da aplicação.

A IoT aproveitou as arquiteturas, tecnologias e protocolos consagrados nos ambientes de TI (existentes na Internet e na WEB) e TELECOM. Assim sendo, muitos mecanismos de segurança da informação puderam ser aproveitados e utilizados tanto no Modelo de Serviços na Núvem com plataformas de serviços prontas (SaaS*(Software as a Service)*, PaaS*(Plataform*

as a Service) e IaaS*(Infrastructure as a Service)*), como nas camadas de protocolos (exemplos : HTTPS, IPSEC, Criptografia na RFID, Segurança do TCP/IP, Criptografia, SSL, TLS, certificados digitais que usam a infraestrutura de chave pública X.509 padrão para associar uma chave pública a uma identidade contida em um certificado. Os certificados X.509 são emitidos por uma entidade confiável chamada CA (Autoridade de Certificação). Esse aproveitamento de protocolos de sucesso e infraestrutura existente na núvem, diminui o investimento e o tempo de desenvolvimento de Softwares Mediadores e Aplicações SMART. É esperado que as plataformas de TI da núvem já possuam mecanismos de segurança embutidos internamente e em seus protocolos de comunicação. Esses mecanismos de Segurança, assim como a Gerência de Rede, são espalhados nas diversas camadas de rede, conforme mostrado na Figura 1.

Os novos protocolos criados para ambientes restritos (*CONSTRAINED*) da IoT utilizam mecanismos de segurança, conforme Tabela 2 que segue. Adicionalmente, apresentam-se as arquiteturas de protocolos para Sensores, Tags, Leitores, Mediadores, Notebooks, Smartphones e Dispositivos : RFID, WiFi, Zigbee e Bluetooth.

Tabela 2 : Mecanismos de Segurança adicionados : a) Protocolos de Acessos Restritos (LIMITAÇÕES (Constrained) em termos de : Potência, Memória, Processador, Banda, Comunicação e Tamanho))
b) Tecnologias de Acesso .

Protocolo/ Arquitetura	**Origem**	**Modelo de Mensagem**	**Mecanismo de Segurança**	**Padronização**	**Transporte**
a) AMQP	Bancos2003	Advertiser/Subscriber	SSL	OASIS 2012	TCP
MQTT	IBM 1999	Advertiser/Subscriber	TLS Brokers (Username + Password)	IEEE 2013	TCP
CoAP	IoT	REST [64] Request/Response Advertiser/Subscriber	DTPLS	RFC 7252	UDP
6LOWPAN	IETF	Micro IP	SubconjuntoIPSEC	RFC4919	IEEE802.15.4
b) RFID	EPCglobal	Tag Information 96bits	Autenticação, Criptografia e Assinatura	GS1 EPCglobal	RFID
WiFi	IEEE	IEEE 802.11 (a,b,g,n)	Criptografia, Filtros MAC, Protocolos e Endereços IPs	IEEE	TCP/IP
ZigBee	ZigBee Alliance	IEEE 802.15/ ISA100.11 a	Controle de Acesso, Criptografia, integridade dos quadros, sequencialidade, Trust Center	IEEE	IEEE802.15.4
Bluetooth	Bluetooth Group	IEEE 802.15.1	Autenticação, Criptografia e Autorização	IEEE	IEEE802.15.4

No nível mais baixo, precisa-se acrescentar mecanismos de segurança nos dispositivos IoT, que são muito numerosos e fonte de informações na qual a funcionalidade do sistema é baseada. A tecnologia RFID já foi criada com endereçamento grande (96 bits) e criptografia na leitura das informações das etiquetas (*TAGs*), sendo assim forte candidata a ocupar este espaço de DISPOSITIVOS de leitura de sensores.

O uso de mecanismos de segurança depende do tipo de aplicação e precisa ser criteriosamente estudado e escolhido, pois implica sempre em aumento de *overhead* e maior atraso e complexidade na comunicação.

a) Proteção de Dados e Mecanismos de Segurança na ***Arquitetura RFID*** da EPCglobal

A análise de segurança depende de cada aplicação, ficando assim sua análise aos proprietários e usuários do sistema baseada na Arquitetura RFID EPCGlobal. A segurança é um processo pelo qual uma organização ou um individuo protege seu acervo de dados, visando reduzir o risco de um ataque.

A RFC 2828 apresenta que a segurança de dados é comumente subdividida em atributos : confidencialidade, integridade, disponibilidade e identificação única (*accountability*). A confidencialidade de dados é uma propriedade que garante que a informação não fique disponível ou revelada para indivíduos não autorizados, entidades ou processos. A integridade dos dados é uma propriedade que os dados não foram alterados, destruídos ou perdidos de forma não autorizada ou de maneira acidental, durante o transporte ou armazenamento. Disponibilidade de Dados é a propriedade de um sistema ou recurso de um sistema ser acessível e ser utilizado sob demanda por uma entidade de sistema autorizado. Identificação Única (*Accountability*) é a propriedade de um sistema que permite que as ações de uma entidade de sistema possa ser identificada unicamente para esse sistema, o qual pode ser responsável por suas ações. As técnicas de segurança como criptografia, autenticação, assinaturas digitais e serviços de não repudio são aplicadas aos dados para prover segurança. A Autenticação é pré-requisito para comunicação criptografada.

Diversas Interfaces de Redes da arquitetura RFID são baseadas em protocolos de arquitetura de rede existentes incluindo as redes TCP/IP. Mecanismos de proteção de dados do protocolo TLS (*Transport Layer Security* – RFC2246 e RFC 4346), permitindo que clientes e servidores selecionem algorítimos de criptografia na troca de certificados, permitindo a autenticação de identidade e compartilhem chaves para permitir a criptografia e o compartilhamento de dados validados. Mecanismos de proteção do protocolo HTTPS (HTTP over TLS : RFC 2818) são utilizados para conteúdo sensível a criptografia para transferência na WEB; pode-se escolher no navegador (*browser*) o uso ou não do TLS (HTTPS ou HTTP). Todos dados HTTP podem ser enviados dentro de conexões TLS ao servidor, protegidas por mecanismos de criptografia negociados durante a conexão TLS. As Aplicações RFID (ALE : *Application Level Events*) podem utilizar o HTTPS provendo autenticação e criptografia, os quais juntos provêm confidencialidade e integridade dos dados compartilhados. Mecanismos de CALLBACK também podem ser utilizados para eventos assíncronos visando garantir a veracidade da comunicação, usando a Operação Segura POST via TLS. O HTTPS permite segurança a nível de link e autenticação mútua opcional. O protocolo entre o Leitor e o Mediador tem opcionalmente a possibilidade de criptografia e autenticação do link de comunicação; mais uma vez o HTTPS pode ser utilizado. Os mecanismos de autenticação X.509 ITU-T podem ser amplamente utilizados para chaves criptográficas.

O Gerenciamento do leitor pode ser feito por meio do uso do protocolo SNMP(RM SNMP MIB, com mecanismos de criptografia e autenticação) ou XML.

O RFID provê 4 modos de segurança : Autenticação de TAGs, Autenticação do LEITOR, Comunicação criptografada (Confidencialidade), e Comunicação com Assinatura (leitores querem receber informações somente de fontes e dispositivos confiáveis). O RFID provê 3 níveis de criptografia : Simples (Tráfego não criptografado), Moderado (Uso do Algorítimo de Criptografia DES) e Avançado (Uso do Algorítimo AES com criptografia de 128 bits).

b) Proteção de Dados e Mecanismos de Segurança no ***Acesso WiFi***

Este tipo de tecnologia de rede é um padrão internacional aberto amplamente utilizada no mundo, possuindo assim mais recursos de segurança. Existem 2 tipos de ataques mais comuns : controle de acesso da rede e segurança de dados. Utiliza-se Autenticação e Criptografia WEP. O WiFi prevê 4 níveis de criptografia : WEP 64 (criptografia de 64 bits), WEP 128 (criptografia de 128 bits), WPA (criptografia de 256 bits) e WPA 2 -PSK (TKIP e AES). O WiFi provê 4 modos de segurança : Projeto de Rede de Modo Seguro, Comunicação Criptografada (WEP, WPA e WPA2), Filtro de Endereços MACs (permite acesso somente de dispositivos desejados), Filtro de Protocolos, desabilitação de Informações SSID de *Broadcast* e Assinalamento de Endereços IPs (Estático ou Dinâmico).

c) Proteção de Dados e Mecanismos de Segurança no ***Acesso ZigBee***

ZigBee é o padrão internacional aberto (ZigBee Alliance) para as redes pessoais PAN (Personal-area networks) visando baixo custo, baixo consumo de potência, confiabilidade, comunicação bidirecional e comunicação sem fio para aplicações de curto alcance. Possui 4 níveis de comunicação : Físico (PHY), Controle de Acesso ao Meio (MAC), Rede (NWK) e Aplicação (APL). Os 2 níveis mais baixo são especificados pelo padrão IEEE 802.15.4, ficando o ZigBee propriamente dito, nas Camadas mais altas (Rede e Aplicação). ZigBee possui uma segurança embutida na própria pilha de protocolo.

A camada MAC possui os seguintes serviços de segurança : Controle de Acesso (*MAC Address*), Comunicação Criptografada usando Chaves Simétricas, Integridade de Quadro por meio de Cheques de Redundância CRC e Sequencialidade de Quadros. Essa camada possibilita 3 modos de operação : Não seguro, Lista de Controle de Acesso com dispositivos permitidos e Seguro. Adicionalmente, o ZigBee também especifica seu próprio modelo de segurança que inclui Estabelecimento de Chave Criptográfica, Transporte de Chave, Proteção de Quadro e Gerenciamento de Dispositivo. A Criptografia no ZigBee pode utilizar chaves de 128 bits ou AES, possuindo 3 tipos de chaves : Chave de Rede (usada por todos os nós da rede), Chave de Link (chaves de sessão secretas, entre dispositivos conectados) e Chave Mestre (usada para gerar a Chave de Link). A chave de Rede já deixa a Rede ZigBee bastante segura pois proíbe que dispositivos não autorizados entrem na rede. O uso do Centro de Controle ZigBee (TC : *Trust Center*) exige que todos os dispositivos para entrar na rede sejam cadastrados e respondam a um único TC. É ele que distribui e armazena as chaves dos dispositivos da rede.

d) Proteção de Dados e Mecanismos de Segurança no ***Acesso Bluetooth***

O Bluetooth é um padrão internacional aberto para comunicação via radio em curtas distâncias, usado também para redes pessoais PAN. Possui os seguintes requisitos de segurança : Autenticação, Criptografia e Autorização. Trabalha com 4 modos de operação : Procedimentos de Segurança não utilizados, Autorização no estabelecimento do link, Autenticação e Criptografia para todas as conexões, e Chave de Link Autenticada e não autenticada. Além dos modos de aparelhamento e autenticação, o Bluetooth provê 3 modos de criptografia : Sem Criptografia, Chaves Criptográficas usadas somente para o tráfego endereçada individualmente (não sendo utilizada para tráfego *broadcast*) e Criptografia usando chave de Link Mestre para todos os tipos de tráfegos.

IV. GERENCIAMENTO DA REDE IoT

O crescimento das redes de transporte e a complexidade dos equipamentos de rede, tratando diversos serviços de rede ao mesmo tempo (voz, dados e vídeo), aumentou o interesse em monitorar e otimizar o uso dessas redes e seus equipamentos e serviços, constituindo assim o PLANO de GERÊNCIA, adicionalmente aos Planos de Dados e de Controle. O Plano de Gerência utiliza o NMS (Network Management System) atuando em regime 24/7 para monitoramento remoto, operação, manutenção e análise de desempenho de redes e equipamentos. O Protocolo SNMP [4], parte da Arquitetura TCP/IP, foi o escolhido como base de comunicação internacional aberta de gerência de redes.

O Gerenciamento e a Supervisão Remota de Equipamentos e Redes foi desenvolvido nos anos 80 para as Redes de Telecomunicações e Redes de TI; teve o objetivo de agilizar a atuação remota em problemas dos equipamentos e redes, os quais passaram a ser acompanhados remotamente, sem pessoal local. Inicialmente utilizava protocolos proprietários para sua execução. Ganhou muita importância mundial, o que levou a órgãos internacionais como ISO, ITU-T e IETF (*Internet Engineering Task Force*) gerassem padronização internacional aberta para essa comunicação. Ganhou ainda maior importância com sua expansão para Gerência de Redes, contemplando novas funcionalidades de Gerência de Falhas, Desempenho e Configuração. Está espalhado por todas as camadas funcionais e camadas de protocolos de comunicação, conforme mostrado na Figura 1. O padrão que se tornou de fato no mundo da Internet foi o SNMP (*Simple Network Management Protocol*) [04] , padronizado pelo IETF por meio da RFC 3584, Gerencia de dispositivos em Redes IPs, ainda muito utilizado atualmente em Servidores, Comutadores(*switches*), Roteadores, Repetidores, *Gateways*, Estação de Trabalho, Impressoras, *racks*, etc; poderá ser utilizado inclusive para dispositivos da IoT. Trabalha com o conceito hierárquico de Gerente/Sub-Agente/Agente atuando sobre os objetos da MIB (*Management Information Base*) com Mensagens dos seguintes tipos : Comando/Resposta(Leitura e Escrita) e Mensagem Espontânea (TRAP). Adicionalmente, possibilita a manipulação de dados por meio do Modelo de Dados MIB, onde os dados são definidos de forma bilateral permitindo seu acesso e modificação.

Especifica (na versão 1) quatro tipos de unidades de dados (PDU) [4]:

1. GET, usado para retirar um pedaço de informação de gerenciamento.
2. GETNEXT, usado interativamente para retirar sequências de informação de gerenciamento.
3. GETBULK, usado para retirar informações de um grupo de objetos.

4. SET, usado para fazer uma mudança no subsistema gerido.
5. TRAP, usado para reportar uma notificação ou para outros eventos assíncronos sobre o subsistema gerido.

No Modelo de Simulação de Rede IoT desenvolvido na Faculdade de Tecnologia da UNICAMP, foram contempladas mensagens do tipo TRAP (do Mediador para a Aplicação SNMP) e COMANDOS/RESPOSTAS (da Aplicação SNMP para o Mediador e depois retornando para a Aplicação SNMP). A taxa de geração das mensagens TRAP e Comandos foi de EXPO [0,6], isto é, 1,67 pacotes/segundo (= 1/0,6) [8].

A Rede IoT também poderá desfrutar do uso do SNMP, pois possuirá equipamentos e elementos a serem supervisionados remotamente. Devido ao grande volume de objetos/coisas/dispositivos a serem supervisionados, é interessante que sejam utilizados elementos MEDIADORES que se preocupem com essa coleta de informação de estado dos dispositivos, além da coleta de informações ambientais dos mesmos. Poderão ser aproveitadas temporariamente soluções proprietárias deste gerenciamento/supervisão.

O Gerenciamento do Leitor pode ser feito por meio do uso do protocolo SNMP(RM SNMP MIB, com mecanismos de criptografia e autenticação) ou XML.

O ZigBee também especifica seu próprio Gerenciamento de Dispositivo.

V. CONCLUSÕES

A IoT é uma nova onda tecnológica que veio complementar a INTERNET tradicional, oferencendo acesso de baixa velocidade/banda para elementos simples de nosso dia-a-dia (*Things*). Foi padronizada internacionalmente, aproveitando as melhores tecnologias já existentes e utilizadas no mercado. Criou diversas Aplicações *SMART* as quais desenvolverão automação de diversos setores da Economia Mundial. A IoT realiza uma nova transformação digital: conecta dispositivos/objetos/coisas, incrementa e automatiza negócios, valoriza processos, redefine organizações e gera uma grande quantidade de oportunidades. É uma nova onda tecnológica com uma nova fronteira para o mundo conectado com as pessoas, dispositivos, ambientes e objetos virtuais, todos conectados e capazes de interação. Isso, com certeza, demandará muitas pesquisas nas redes mundiais globalizadas e em suas aplicações. As áreas de Segurança e Gerenciamento de Rede são muito importantes para esse tipo de rede, sendo assim as mais detalhadas neste artigo.

REFERÊNCIAS

[1] Recomendações Série Y.4000/Y.2060 : Overview of the Internet of things. ITU-T Genebra 2016. Obs. Standards prepared on a collaborative basis with ISO and IEC;

[2] Provided security measures of enabling technologies in Internet of Things (IoT): ASurvey;Minela Grabovica; Srđan Popić; Dražen Pezer; Vladimir Knežević;Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016; IEEEE 2016.

[3] Security architecture for mobile e-health applications in medication control; Fabio Gonçalves; Joaquim Macedo; M. João Nicolau; Alexandre Santos; Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on; IEEE 2013.

[4] Essential SNMP; Douglas R.Mauro, Kevin J.Schmidt, O'Relly 2005.

[5] Internet of things network management system architecture for smart healthcare;Farag Sallabi; Khaled Shuaib;Digital Information and Communication Technology and its Applications (DICTAP), 2016 Sixth International Conference on; IEEE 2016;

[6] Management and Internet of things. Mayara Smaniego; Ralph Deters; The 13th International Conference on Mobile Systems and Pervasive Computing (MobSPC 2016).

[7] How to Create an Effective Information Security Risk Managementt Program; Llia Sotnikov; Cyber Chief Magazine, June 2019.

[8] A Validation Method for Adhoc Network Simulation including MANETS, VANETS and Emergency Scenarios. José Roberto Emiliano Leite, Edson L. Ursini, Paulo S. Martins. ADHOC NOW 2019 Luxemburgo, Outubro/2019.