Internet of Things: A Survey on Communication Protocol Security

Walter E. Santo
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
walterdoespiritosanto@gmail.com

Ricardo J. P. de B. Salgueiro
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
salgueiro@ufs.br

Reneilson Santos
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
reneilson1@gmail.com

Danilo Souza
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
danilosilva.se@gmail.com

Admilson Ribeiro
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
admilson@ufs.br

Edward Moreno
Universidade Federal de Sergipe
Sao Cristovao, Sergipe
edwdavid@gmail.com

ABSTRACT

This paper presents a survey on the main security problems that affect the communication protocols in the context of Internet of Things, in order to identify possible threats and vulnerabilities. The protocols RFID, NFC, 6LoWPAN, 6TiSCH, DTSL, CoAP and MQTT, for a better organization, were explored and categorized in layers according to the TCP / IP reference model. At the end, a summary is presented in tabular form with the security modes used for each protocol is used.

CCS CONCEPTS

• **Networks** → Network protocols; Security protocols; Cyber-physical networks; • **General and reference** → Surveys and overviews;

KEYWORDS

Internet of Things, Vulnerabilities, Security, IoT Protocols, Survey

ACM Reference Format:
Walter E. Santo, Ricardo J. P. de B. Salgueiro, Reneilson Santos, Danilo Souza, Admilson Ribeiro, and Edward Moreno. 2018. Internet of Things: A Survey on Communication Protocol Security. In *Euro American Conference on Telematics and Information Systems (EATIS '18), November 12–15, 2018, Fortaleza, Brazil.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3293614.3293644

1 INTRODUÇÃO

A Internet das Coisas, do inglês: Internet of Things (IoT), denominação sugerida por Kevin Aston, é uma revolução tecnológica em computação e comunicações que retrata uma variedade de dispositivos inteligentes amplamente interconectados [17] e tem uma entidade digital [10]. Os dispositivos são capazes de interpretar e reagir ao ambiente graças à combinação da Internet com tecnologias emergentes como a Identificação por Radiofrequência (RFID) [7], localização em tempo real e sensores embarcados. Até 2020, estima-se que 13.5 bilhões de dispositivos estarão conectados [4].

O aumento do número de dispositivos IoT deve ser acompanhado por uma infraestrutura capaz de suportar a enorme quantidade de tráfego, armazenamento e processamento dos dados, de maneira eficiente e segura. Conhecer quais são os protocolos e suas principais características é extremamente importante ao se projetar a arquitetura do ambiente IoT, de modo a garantir sua segurança. Falhas de transmissão, negação de serviço, interceptação dos dados, ataques de autenticação, *spoofing*, entre outros, podem vir a acontecer caso a escolha do protocolo não esteja condizente com as especificações e limitações dos dispositivos e das diversas interfaces com as quais eles se comunicam. Uma comunicação segura envolve confidencialidade, integridade, autenticação e não-repudio, que podem ser endereçadas pelos protocolos ou por mecanismos externos [12]

Neste trabalho, é fornecido um *survey* com ênfase nas principais características e garantias de segurança com baixo consumo computacional nos protocolos de comunicação da Internet das Coisas, alertando para possíveis vetores de ataque. Este está estruturado em cinco seções: a Seção 2 exibe trabalhos relacionados; Seção 3 apresenta a segurança nos principais protocolos IoT; a Seção 4 é dedicada à síntese de segurança dos protocolos; por fim, na Seção 5 tem-se as conclusões, com sugestões de trabalhos futuros.

2 TRABALHOS RELACIONADOS

Estudos relacionados à área de segurança tentam fornecer variados levantamentos em diferente aspectos relacionados a segurança e protocolos de comunicação em IoT.

Lin et. al [14], discutem como a IoT pode se beneficiar com o uso da *Fog Computing* e apresentam uma abrangente pesquisa de esforços recentes sobre arquiteturas, tecnologias facilitadoras e questões de segurança e privacidade. Yang et. al em [26] exploram a segurança em IoT do ponto de vista da limitação dos dispositivos, autenticação e controle de acesso. Além disso, os autores apresentam a classificação de diferentes ataques e discutem perspectivas da segurança em diferentes camadas da arquitetura IoT. Ammar et al. [9], apresentam uma análise comparativa dos principais frameworks de IoT para sustentar o argumento de que o sucesso no desenvolvimento de aplicações IoT depende principalmente das questões relacionadas à segurança e privacidade. Os resultados da comparação apontam que as arquiteturas de segurança utilizam

EATIS '18, November 12–15, 2018, Fortaleza, Brazil

ACM ISBN 978-1-4503-6572-7/18/11…$15.00
https://doi.org/10.1145/3293614.3293644

padrões de proteção semelhantes embora adotem metodologias diferentes. O trabalho apresentado por [15], discute aspectos do uso de *middlewares* para IoT. Não obstante, os autores apresentam uma análise dos desafios e das tecnologias capacitadoras no desenvolvimento de um *middleware* IoT considerando aspectos como heterogeneidade de dispositivos, adaptabilidade e segurança.

Diferente dos recentes esforços de pesquisa à respeito segurança em IoT, o presente trabalho dá ênfase em aspectos de segurança dos principais protocolos IoT e suas camadas, bem como, discute a implementação da segurança e diferentes tipos de ataques.

3 SEGURANÇA NOS PROTOCOLOS IOT

Os principais problemas de segurança em IoT envolvem questões relativas à privacidade, portanto, devem ser orquestradas soluções para estes problemas a partir da estipulação de protocolos [23], que ofereçam mecanismos de segurança ao mesmo tempo que fornecem a agilidade e escalabilidade necessária para o fluxo de dados [16].

Quando se trata de IoT, diversos fatores influenciam a escolha dos protocolos a serem utilizados. Tempo de vida da bateria, *Ligthweight Computation* [26], necessidades da troca de dados, alcance mínimo e máximo, mobilidade dos nós na rede, taxas de perda e de erro, comunicação com a nuvem, entre outros. Além de utilizar os protocolos já conhecidos da Internet convencional como TCP/IP, HTTP/REST, WiFi e Ethernet, novos protocolos ganham importância, principalmente nas camadas físicas e de enlace, nas quais os dispositivos, conectados a sensores, formam as RSSF (Redes de Sensores sem Fio) e passam a possuir restrições energéticas e de processamento.

Para o presente estudo, os protocolos foram categorizados de acordo com as camadas as quais pertencem. A Tabela 1 ilustra o posicionamento dos protocolos que são abordados de acordo com suas camadas principais no modelo de referência TCP/IP.

Table 1: Categorização dos protocolos em camadas segundo o modelo TCP/IP

Modelo de referência TCP/IP	Protocolos
4- Aplicação	CoAP, MQTT
3- Transporte	DTLS
2- Rede	6loWPAN, 6TiSCH
1- Física/Enlace	RFID, NFC

3.1 Camada Física e de Enlace: RFID e NFC

Considerado como base fundamental para a definição do que é a Internet das Coisas, a identificação por rádio frequência (RFID) [8], se apresenta como uma solução para o endereçamento único de dispositivos. Funciona pela emissão de ondas eletromagnéticas por leitores que, por sua vez, ativam as etiquetas, que contêm informações elétricas armazenadas e as transmitem por uma antena. Tais etiquetas podem ser passivas (ativadas no momento em que recebem o estímulo da onda eletromagnética), ou ativas (ligadas a uma fonte de energia, possuindo, por conseguinte, um alcance maior). Os principais aspectos de segurança dos protocolos de baixo custo utilizados para o RFID, segundo [27] são: confidencialidade, integridade, disponibilidade, autenticidade e privacidade.

O *Near Field Communication* (NFC) [11], é um conjunto de protocolos para a comunicação de dispositivos fisicamente próximos através de campo eletromagnético (incluindo o RFID). Entretanto, o NFC é definido apenas para objetos com aproximadamente 10cm de distância e não possui restrições quanto à direcionalidade da comunicação (uma etiqueta pode se comportar como um leitor e o leitor como etiqueta), possibilitando uma comunicação ponto a ponto [1]. A principal utilização do NFC tem sido para pagamentos sem cartão.

Definido pelo padrão ISO-14443, o protocolo NFC possui três fases principais: (i) Evitar Colisão de RF (Rádio Frequência) – o Leitor só ativa sua RF quando nenhuma outra RF tiver sido detectada; (ii) Detecção de Dispositivo – o Leitor sonda alvos próximos e recebe uma resposta em determinado intervalo de tempo (*time-slot*); e (iii) Protocolo de Transporte – após ter encontrado um alvo, o Leitor inicia a transmissão utilizando do protocolo de transporte, o qual especifica parâmetros como o *timeout* esperado [6].

A Tabela 2 traz uma lista dos principais e mais comuns ataques aos protocolos RFID e NFC.

Table 2: Principais e mais comuns ataques aos protocolos RFID e NFC

Tipo de ataque	Descrição
Eavesdropping	Ocorre quando um espião consegue ter acesso à informação transmitida entre uma etiqueta e um leitor.
Ataques *Man-In-The-Middle*	Um atacante entre um servidor e uma etiqueta recebe os dados da comunicação sendo realizada.
Ataques de *Replay*	São proporcionados por atacantes que têm acesso a um dado transmitido e o repassa com *spoofing* da identificação da etiqueta e também para ataques *Man-in-the-middle.*
Ataques de Desincronização	Um tipo de ataque de negação de serviço em que a informação relativa a uma etiqueta armazenada em um servidor é confundida com a informação que está armazenada na etiqueta, inviabilizando a comunicação.
Ataques de Personificação	Um atacante faz uso da identificação da etiqueta para se autenticar em um servidor.
Ataques de Negação de Serviço (DoS)	É adicionado ruído de modo a interromper a operação normal do RFID.
Jamming físico	Funciona como um ataque de DoS, ao se transmitir sinais de rádio que impõem ruído ao sinal transmitido.

3.2 Camadas de Rede: 6LoWPAN e 6TiSCH

Como não é possível se estabelecer uma integração direta entre o IPv6 e o IEEE 802.15.4 [1], o grupo IPv6 sobre redes sem-fio de baixa potência em PANs, do inglês *IPv6 over Low-power Wireless*

[1]O protocolo IEEE 802.15.4 define quais são as condições necessárias para a comunicação entre dispositivos com baixo consumo energético e de pouco alcance, as *Low-power Wireless Personal Area Network* (LoWPAN)

Personal Area Networks (6LoWPAN)[13], busca mecanismos para o desenvolvimento de uma pilha de protocolos que forneça essa integração. Técnicas como compressão de cabeçalho, fragmentação e reestruturação de pacotes, descoberta de vizinhos e autoconfiguração são utilizadas na adequação do protocolo IPv6 para as redes sem fio de baixa potência em WPANs.

O 6LoWPAN, então, define uma nova camada de adaptação entre a camada de rede e de enlace (*6LoWPAN Adaptation Layer*), na qual é realizada: a fragmentação e reconstrução dos pacotes enviados, que não podem ser fragmentados pelo IPv6; a compressão do cabeçalho e o roteamento para a camada de enlace. Granjal et al. em [12] ressalta que não são implementados mecanismos de segurança específicos para o 6LoWPAN, visto que este conta com a segurança a nível de enlace provida pelo protocolo IEEE 802.15.4. O fato de não estar autenticado, permite que atacantes explorem vulnerabilidades no processo de fragmentação, no qual deve ser mantido um *buffer* para a remontagem dos pacotes. Também, como os dados não são criptografados, em [18] afirma-se que o 6LowPAN está vulnerável a ataques de *eavesdropping*, *man-in-the-middle* e *spoofing*.

Um estudo realizado por Vohra e Srivastava em [25] elicita trabalhos de pesquisa de vulnerabilidades no 6LoWPAN e técnicas para a segurança no mesmo, porém, não se mostrou, até o momento, adequada para redes de baixo custo energético e de processamento. Ainda para a integração, o grupo 6TiSCH busca integrar o IPv6 com a versão IEEE 802.15.4e. Nele, é realizada a divisão de tempo TDMA (Acesso Múltiplo por Divisão de Tempo), em que uma faixa de banda é definida para a comunicação entre nós vizinhos [3].

3.3 Camada de Transporte: DTLS

O TLS é o protocolo utilizado para garantir segurança na Internet, desde aplicações bancárias até trocas de mensagens instantâneas, porém tem um alto custo computacional para ser implementado e não foi desenvolvido para aplicações de tempo crítico [11]. O DTLS (*Datagrama Transport Layer Security*) se apresenta como um protocolo para trazer a segurança na comunicação de datagramas pela rede através do UDP, que é menos confiável para a entrega de pacotes, porém permite um maior fluxo de dados, para superar o problema de tempo crítico. O DTLS é uma alternativa viável ao TLS no que se refere à transferência de dados pela Internet de Redes de Sensores Sem Fio (RSSF) conectadas. Apesar de ter sido desenvolvido para superar questões relativas ao tempo-crítico na Internet convencional, como no caso de games, por exemplo, o protocolo DTLS ganha especial importância para IoT.

O TLS funciona sobre quatro outros protocolos: (1) *Record Protocol*; (2) *Handshake Protocol*; (3) *Alert Protocol* e (4) *Change Cipher Spec*. [12].

Um estudo exposto no RFC 7457[2] traz as principais vulnerabilidades conhecidas para o TLS e DTLS [20] - *stripping*; injeção de comandos STARTTLS; ataque BEAST; ataque *padding oracle*; ataques no RC4; ataques de compressão: CRIME, TIME, e *Breach*; ataques de certificado e RSA; parâmetros *diffie-hellman*; roubo de chaves privadas do RSA; renegociação; ataque de *handshake* triplo; confusão do hospedeiro Virtual; negação de serviço (DoS); problema de implementação e problema de usabilidade.

[2]RFC (*Request for Comments*) 7457 <https://tools.ietf.org/html/rfc7457>

Versões antigas do TLS devem ser evitadas, pois são consideradas inseguras. Atualmente, a versão 1.2, tanto do TSL como DTLS, são preferíveis, e é importante não deixar que o protocolo caia de versão, processo que pode ser ativado por um ataque *Man-In-The-Middle*, colocando o sistema em posição instável, dada a insegurança das versões antigas [20].

3.4 Camada de Aplicação: CoAP e MQTT

Definido pela IETF (*Internet Engineering Task Force*), o CoAP (*The Constrained Application Protocol*) [21] representa o protocolo de camada de aplicação para redes e nós com restrições. É definido para aplicações M2M (*Machine to Machine*) e assemelha-se ao HTTP. Utiliza comandos GET, PUT, POST e DELETE, do modelo REST, e faz uso de conceitos da web como URIs [2]. A implementação do CoAP, porém, se comporta tanto como servidor como cliente em uma comunicação M2M.

O CoAP é dividido em duas camadas, uma que lida com requisições e respostas e outra para tratar as mensagens sendo transmitidas pelo UDP. Existem quatro possíveis tipos de mensagem no CoAP: (1) *Acknowledgement* (ACK), para sucesso; (2) *Reset*, para rejeitar uma mensagem confirmável ou remover um observador; (3) Confirmável, indica uma entrega confiável da mensagem e (4) Não-Confirmável, não espera uma confirmação do envio. Como está sobre o UDP, em que a entrega não é garantida, a transmissão pode exigir confirmação de entrega, por isso mensagens do tipo confirmável sempre retornam um ACK quando bem-sucedidas [19]. Assim como no HTTP, o CoAP possui sua série de códigos e mensagens de resposta [12].

Para a segurança, o CoAP utiliza do DTLS, logo, transfere para a camada de transporte a manipulação de mecanismos de segurança [12]. O protocolo provê quatro modos de segurança: (1) *NoSec*: nenhum mecanismo de segurança do DTLS é aplicado, (2) *PreSharedKey*: utilizado com dispositivos que já são pré-programados com as chaves simétricas necessárias, onde cada chave possui uma lista de nós que podem se comunicar, (3) *RawPublicKey*: o dispositivo possui um par de chaves assimétricas sem a utilização de certificado, que é validado por um mecanismo *out-of-band* e (4) *Certificate*: o protocolo faz o uso do DTLS com um certificado X.509, o dispositivo possui também usa uma lista de raízes confiáveis [12, 21].

A Tabela 3 traz as possíveis ameaças ao protocolo CoAP de acordo com o RFC 7252 [21].

O MQTT (*Message Queuing Telemetry Transport Protocol*), desenvolvido em 1999 originalmente pela IBM, se tornou um padrão aberto ISO (ISO/IEC 20922:2016) [5]. Trata-se de um protocolo, leve e simples de implementar, para o enfileiramento e transporte de mensagens, que se utiliza do modelo *publish/subscribe*. Seus componentes principais são: *brokers*, sessões, assinaturas (*subscriptions*) e assunto (*topic*) [22].

O modelo *publish/subscribe* envolve a definição de um comunicante e de diversos ouvintes, conectados em um *broker*, que organiza a troca de mensagens entre assinantes e publicantes. O assinante registra o interesse em determinado assunto e, assim que algum publicante disponibiliza conteúdo neste tópico, o *broker* direciona a mensagem para os assinantes registrados. A qualidade de serviço nesse processo é dividida em três categorias: (1) No máximo uma vez (*At most once/Fire and Forget*), que utiliza do melhor esforço

Table 3: Ameaças ao protocolo CoAP – RFC 7252

Tipo de ataque	Descrição
Parsing do Protocolo e Processamento de URIs	É possível explorar vulnerabilidades no processo de *parsing* (processo que analisa uma sequência de entrada), para, por exemplo, gerar um ataque de negação de serviço ao se inserir um texto que irá acarretar em parser muito extenso.
Proxying e *Caching*	O *proxy* é, por si só, um *man-in-the-middle*, quebrando toda segurança do IPSec e DTLS. Ameaças são amplificadas quando os *proxies* permitem que haja uma cache dos dados.
Risco de Amplificação	As respostas no CoAP são, geralmente, maiores do que as requisições, o que pode facilitar ataques por amplificação.
Ataques de IP *Spoofing*	Como não há *handshake* para o UDP, o nó final que possui acesso à rede pode realizar *spoofing* para enviar mensagens de ACK no lugar de CON, prevenindo que haja retransmissão; *spoofing* em todo o *payload*; *spoofing* de pedidos *multicast*; etc.
Ataques *Cross-Protocol*	Envolvem utilizar o CoAP para enviar ataques a outros protocolos, para se passar pelo *firewall*, por exemplo.
Nós com Restrições	Sejam restrições energéticas, de memória ou de processamento, dificultam que os dispositivos disponham de boa entropia. Assume-se, portanto, que os processos que necessitem de entropia, como o cálculo de chaves, o façam externamente.

para se enviar, caso não chegue em determinado envio pode chegar no próximo; (2) Ao menos uma vez (*At least once*), garante que a mensagem chega, mas pode ocorrer duplicatas e (3) Exatamente uma vez (*Exactly once*), que garante que a mensagem chegará e não irão ocorrer duplicatas [22].

Assim como no CoAP, a segurança é endereçada por fora, pelo TLS, que é muito pesado para os dispositivos IoT. Em [24] é proposto um modelo de aplicação seguro para o MQTT, denominado SMQTT, por meio de criptografia baseada em atributo leve (*Lightweight* ABE), que provê criptografia por *broadcast*, sobre curvas elípticas. Esse modelo, segundo os autores, se mostrou resistente a ataques de *plaintext* conhecido, *ciphertext* conhecido e de *man-in-the-middle*.

4 SÍNTESE DE SEGURANÇA DOS PROTOCOLOS

O presente trabalho teve seu foco principal na abordagem da segurança dentro dos principais protocolos de comunicação IoT, identificando as respectivas vulnerabilidades e ameaças. Nessa direção, como resultado do estudo criou-se uma compilação dos possíveis tipos de ataques e dos modos de segurança empregados em cada protocolo, conforme apresentado na Tabela 4. Um agrupamento geral, reunindo as ameaças mais recorrentes, comuns aos principais protocolos, classificaram estes de acordo com as camadas a que pertenciam. No decorrer da pesquisa, observou-se a ausência de dados compilados dessa natureza, de fácil acesso e manipulação, voltados para segurança em IoT. Por conseguinte, o resultado desse estudo tem como principal diferencial fornecer um material consistente para pesquisas futuras, possível de ser enriquecido e complementado ao longo do processo de consolidação da IoT, agregando novos protocolos com suas respectivas vulnerabilidades.

4.1 Tipos de Segurança Implementados

A Tabela 4 apresenta um resumo dos modos de segurança implementados em cada protocolo, que foram descritos na Seção 3. Na tabela, AAA se refere a Autenticação, Autorização e Prestação de Contas, do inglês *Authentication, Authorization and Accountability* e a confidencialidade descreve os cifradores que o protocolo utiliza.

Table 4: Resumo dos modos de segurança implementados

Protocolo	Modos de segurança	AAA e Integridade	Confidencialidade
6loWPAN / 6TiSCH	Não implementa segurança	-	-
DTLS	*Record Protocol, Handshake Protocol, Alert Protocol, Change Cipher Spec*	HMAC-SHA1, HMAC-SHA256/ 384 e AEAD	Possui vários cifradores que podem ser selecionado
COAP	*No Sec*, *PreSharedKey*, *Raw Public Key* e *Certificate*	Lista de Raízes Confiáveis, Utiliza o DTLS	AES-CCM
MQTT	Utiliza o DTLS	Campo para o nome e senha utiliza DTLS	Utiliza DTLS

4.2 Tipos de Ataques Identificados

Vários ataques e vulnerabilidades foram identificados em cada protocolo. A Tabela 5 traz os ataques comuns em cada camada, na qual, caso tenha sido identificado no trabalho, o ataque é marcado. Em alguns casos, são feitas observações, dado que certos ataques só ocorrem quando mecanismos de segurança não são aplicados.

A camada física e de enlace, dada a abertura na qual a comunicação sem fio apresenta, está suscetível a diversos ataques. Entretanto, existem diversas soluções para tentar mitigar tal vulnerabilidade, porém, é intrínseco do ambiente que tais ataques possam ser aplicados. O *jamming*, por exemplo, pode ocorrer também na camada de enlace. Ao se transmitir informação sem criptografia em redes sem fio, qualquer indivíduo pode ter acesso a ela.

Na camada de rede foram identificados diversos ataques comuns dentro do processo de roteamento. Os ataques DoS ganham especial relevância no ambiente de IoT pois visam esgotar a bateria dos dispositivos. Aplicar o IPv6 nesse ambiente é também uma tarefa complexa, que envolve a compressão e fragmentação e pode, consequentemente, dar espaço a ataques.

O DTLS foi colocado na camada de transporte, apesar do mesmo ser uma adaptação para segurança entre as camadas de aplicação

Table 5: Ataques que podem ser explorados nos protocolos por camada

Camada	Protocolo	Aplicação																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Aplicação	CoAP																X	X**	
	MQTT																	X**	X**
Transporte	DTLS	X					X		X		X	X	X		X	X			
Rede	6loWPAN		X		X			X		X				X					
Física e Enlace	RFID e NFC		X*	X	X	X			X										

*Modos de segurança sem Criptografia. **CoAP, MQTT, estão vulneráveis a certos ataques somente quando não utilizam DTLS. 1- SSL Stripping, RC4, Problema de Usabilidade; 2- *Eavesdropping*; 3- *Relay*; 4- *Man-in-the-Midle*; 5- *Jamming* físico; 6- Injeção de Comandos; UDP *Flooding*; 7-*Spoofing*; 8- DoS; 9- Fragmentação; 10- CRIME, TIME, *Breach*, Parâmetro *Diffie-Hellman*; 11- BEAST, *Passing Oracle*, Problema de Implementação; 12- Roubo de Chaves do RSA, Certificado RSA; 13- *Realy Attack*; 14- *Handshake* Triplo, Renegociação; 15- Confusão de Hospedeiro Virtual; 16- Amplificação; 17- *Masquerading*; 18- *Trashing*;

e de transporte. Consideram-se, então, como vulnerabilidades da camada de transporte as vulnerabilidades do DTLS.

Dos protocolos da camada de aplicação, poucos possuem segurança embutida como padrão. A maioria se utiliza da segurança provida pelo DTLS. Cabe ao administrador da rede e desenvolvedores verificar a sensitividade dos dados e as restrições dos nós para implementar corretamente a segurança. Vale ressaltar que as ameaças desta camada são mais relacionadas ao software da aplicação do que aos protocolos em si.

5 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho, ao abordar aspectos relevantes voltados para segurança em IoT, trouxe uma visão macro da necessidade urgente de serem adotadas medidas para mitigar vulnerabilidades e ameaças, em sua maioria, do tipo DoS. Identificou-se as principais ameaças existentes e foram apresentadas algumas sugestões para evitá-las. Foi possível, então, agrupar as ameaças encontradas por camada de acordo com a atuação de cada protocolo. Como trabalhos futuros, um possível estudo, seria aplicar o mesmo método de pesquisa adotado neste artigo aos protocolos *Bluetooth*, BLE, IEEE 802.15.4, *Z-Wave*, *Wifi Direct* e LTE-A.

REFERENCES

[1] [n. d.]. RFID vs. NFC: What's the Difference? http://blog.atlasrfidstore.com/rfid-vs-nfc

[2] 2011. Coap Technology. Retrieved 15/05/2017 from http://coap.technology/

[3] 2011. IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch). Retrieved 18/05/2017 from https://datatracker.ietf.org/wg/6tisch/charter/

[4] 2015. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. Retrieved 07/05/2017 from https://www.gartner.com/newsroom/id/3165317

[5] 2016. Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1. Retrieved 19/06/2017 from http://www.iso.org/iso/catalogue_detail.htm?csnumber=69466

[6] Nikolaos Alexiou, Stylianos Basagiannis, and Sophia Petridou. 2016. Formal security analysis of near field communication using model checking. *Computers & Security* 60 (2016), 1–14.

[7] Leonardo A Amaral, Fabiano P Hessel, Eduardo A Bezerra, Jerônimo C Corrêa, Oliver B Longhi, and Thiago FO Dias. 2011. eCloudRFID–A mobile software framework architecture for pervasive RFID-based applications. *Journal of Network and Computer Applications* 34, 3 (2011), 972–979.

[8] Sara Amendola, Rossella Lodato, Sabina Manzari, Cecilia Occhiuzzi, and Gaetano Marrocco. 2014. RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of things journal* 1, 2 (2014), 144–152.

[9] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* 38 (2018), 8–27.

[10] Jordán Pascual Espada, Oscar Sanjuán Martínez, Juan Manuel Cueva Lovelle, B Cristina Pelayo G-Bustelo, Manuel Álvarez Álvarez, and Alejandro González García. 2011. Modeling architecture for collaborative virtual objects based on services. *Journal of Network and Computer Applications* 34, 5 (2011), 1634–1647.

[11] Roy Fisher and Gerhard Hancke. 2014. DTLS for lightweight secure data streaming in the internet of things. In *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on*. IEEE, 585–590.

[12] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1294–1312.

[13] Nurul Halimatul Asmak Ismail, Rosilah Hassan, and Khadijah WM Ghazali. 2012. A study on protocol stack in 6lowpan model. *Journal of Theoretical and Applied Information Technology* 41, 2 (2012), 220–229.

[14] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal* 4, 5 (2017), 1125–1142.

[15] Anne H Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z Sheng. 2017. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal* 4, 1 (2017), 1–20.

[16] Kim Thuat Nguyen, Maryline Laurent, and Nouha Oualha. 2015. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks* 32 (2015), 17–31.

[17] Ismael Peña-López et al. 2005. ITU Internet report 2005: the internet of things. (2005).

[18] Pavan Pongle and Gurunath Chavan. 2015. A survey: Attacks on RPL and 6LoWPAN in IoT. In *Pervasive Computing (ICPC), 2015 International Conference on*. IEEE, 1–6.

[19] Reem Abdul Rahman and Babar Shah. 2016. Security analysis of IoT protocols: A focus in CoAP. In *Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on*. IEEE, 1–7.

[20] Yaron Sheffer, Ralph Holz, and Peter Saint-Andre. 2015. *Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS)*. Technical Report.

[21] Zach Shelby, Klaus Hartke, and Carsten Bormann. 2014. *The constrained application protocol (CoAP)*. Technical Report.

[22] Shubhangi A Shinde, Pooja A Nimkar, Shubhangi P Singh, Vrushali D Salpe, and Yogesh R Jadhav. 2016. MQTT-message queuing telemetry transport protocol. *International Journal of Research* 3, 3 (2016), 240–244.

[23] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks* 76 (2015), 146–164.

[24] Meena Singh, MA Rajan, VL Shivraj, and P Balamuralidhar. 2015. Secure mqtt for internet of things (iot). In *Communication systems and network technologies (CSNT), 2015 fifth international conference on*. IEEE, 746–751.

[25] Saniya Vohra and Rohit Srivastava. 2015. A survey on Techniques for Securing 6LoWPAN. In *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 643–647.

[26] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. 2017. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal* 4, 5 (2017), 1250–1258.

[27] Azam Zavvari and Ahmed Patel. 2012. Critical evaluation of RFID security protocols. *International Journal of Information Security and Privacy (IJISP)* 6, 3 (2012), 56–74.