Segurança e Privacidade para IoT Aplicadas a Saúde

Interconexão segura e protocolos para IoT no contexto de eHealth

Euclides Palma Paim
Programa Interdisciplinar de Pós-Graduação em Computação Aplicada
Universidade do Vale do Rio dos Sinos - Unisinos
São Leopoldo, Brasil
euclidespaim@gmail.com

***Abstract*—Internet of Things or IoT is characterized by a highly interconnected network of multiples devices with a heterogeneous nature which have capabilities to connect physical objects into a unified system. Nonetheless the dynamic of these environments may facilitate the unauthorized access to the networks. Related to the eHealth context these concerns are magnified as well the intrinsic features of information than the critically aspects of the activity. In this paper we will describe these features, analyze the risk of these operation and the solution available to mitigate de treats in wireless sensor networks and wireless body area networks.**

***Index Terms*—Iot, security, privacy, protocols, WSN, WBAN, eHealth.**

I. Introdução

O que conhecemos hoje como IoT (*Internet of Things*) é um conceito que vem se desenvolvendo a pelo menos trinta anos. Mark Weiseir [1] disseminou a ideia no começo dos anos 90 e Kevin Ashton [2] cunhou o termo que é utilizado até hoje, em uma apresentação para executivos no final dessa mesma década. Com o franco desenvolvimento dessa área estima-se que em torno de 26 bilhões de "coisas," excluindo computadores pessoais, *smartphones* e *tablets*, conectem-se a *internet* até 2020, um avanço médio de 25% ao ano segundo o instituto de pesquisas Gartner [3].

Existem diversos campos de aplicação para tecnologias IoT e seu uso voltado para a saúde é um exemplo, onde podem ser aplicadas ao contexto hospitalar *eHealth* para monitoramento de pacientes, diagnóstico de doenças e controle da cadeia de suplementos médicos.

Os recentes avanços tecnológicos em comunicação sem fio, sistemas eletrônicos miniaturizados, circuitos de baixa potência e sensores, invasivos ou não, voltados para o contexto de eHealth permitem a criação das chamadas *Wireless Body Area Networks* (WBANs). Esse conjunto de dispositivos compõem sistemas que podem reduzir o tempo de reação de médicos e enfermeiras, aproximar paciente e equipe médica e ainda facilitar o acompanhamento destes além dos hospitais e clínicas *Homecare*.

Formando um ambiente heterogêneo permeado por múltiplos protocolos, camadas de rede e uma quantidade crescente de dispositivos conectados é essencial que esses sistemas mantenham um alto nível de disponibilidade, qualidade de serviço, segurança e privacidade. Sensores, s*martphones*, etiquetas RFID e servidores que se comunicam principalmente por redes *wireless* ampliam preocupações relacionadas à segurança e a privacidade. A utilização de aparelhos com pouca ou nenhuma capacidade de processamento e a natureza das redes de baixa frequência desafia a confidencialidade e integridade da informação. Para garantir a precisão de diagnósticos apoiados por essa tecnologia, as tradicionais medidas de segurança não podem ser aplicadas diretamente e novas estratégias devem ser adotadas.

Nesse sentido este *survey* é um esforço para analisar os principais estudos disponíveis atualmente para minimizar ameaças e avaliar os riscos evolvendo segurança e a privacidade em *eHealth*. Identificar os protocolos conhecidos de criptografia e avaliar os desafios à segurança e privacidade em *Wireless Sensor Network* (WSN), *Wireless Body Area Networks* (WBAN) e *Biomedical Sensor Networks* (BSN).

A contribuição deste artigo pode ser vista na tabela 2 onde são relacionados os trabalhos conhecidos comparados as questões abordadas neste *paper*. As demais seções deste *survey* mostram os trabalhos disponíveis, a seção 2 descreve os aspectos referentes à arquitetura e visão geral relacionada a segurança. Estudos conhecidos relacionados à privacidade são analisados na seção 3. O capítulo 4 aborda protocolos de comunicação seguros utilizados em WSN e WBAN com ênfase para utilização em aplicações voltadas a saúde. E conclusão discute as questões em aberto relacionadas ao assunto para possíveis pesquisas futuras.

II. Estrutura e Segurança Visão Geral

IoT é uma área com grande potencial para aplicação nos serviços de saúde. Onde sistemas eletrônicos de saúde são baseados em redes sem fio e frequências de rádio que possibilitam o monitoramento em tempo real de sensores. Estes estrategicamente distribuídos em pacientes ou ao redor deles, geram um fluxo de informações que vai facilitar as rotinas hospitalares, diminuir o tempo de procedimentos e reduzir custos inerentes ao processo. Estas informações são, na sua origem, particulares e qualquer falha de privacidade ou na credibilidade dos dados transmitidos, pode gerar desconfiança

ou preconceito por parte de pacientes a respeito dessa tecnologia.

TABLE I. ABREVIATURAS E NOTAÇÕES

Abreviaturas	Definição
IoT	Internet of Things
WSN	Wireless Sensor Network
WBAN	Wireless Body Area Network
BSN	Body Sensor Network
IDS	Intrusion Detecion System
6LoWPAN	Low Power Personal Area Network
6LBR	6LoWPAN Border Router
KMS	Key Management System
PKC	Public Key Cryptography
IBE	Identify-based Encryption
ABE	Attribute-based Encryption
DTLS	Datagram Transport Layer Security
IFC	Information Flow Control
PPDM	Privacy Preserving Data Mining

a. Abreviaturas e notações utilizadas ao longo do artigo.

Aplicações voltadas para eHealth são essencialmente conscientes do contexto, dinâmicas e pessoais [5]. Dados relacionados à saúde são especialmente sensíveis, segundo [6] IoT estão mais vulneráveis a ataques físicos que outras aplicações de rede. Assim tomar medidas que garantam a confidencialidade das informações que circulam por esses sistemas deve ser o objetivo desde o inicio de um projeto que envolva ou adote soluções aplicadas a esse conceito.

Nos artigos analisados observa-se os esforços de pesquisadores a fim de responder questões referentes a:

- Como garantir acesso seguro a ambientes onde máquinas e seres humanos competem por autenticação?
- É prudente reutilizar os mecanismos de segurança tradicionais?
- Que tipo de chaves de autenticação em uso são mais eficientes para ambientes inteligentes IoT?
- As informações que estão sendo transmitidas pela rede de sensores são confiáveis e corresponde a realidade?

A. Estrutura IoT e Aspectos de Segurança

Atualmente para cada área de aplicação IoT são adotados padrões diferentes e não há uma estrutura comum relacionada a segurança [8]. Apesar de diversas pesquisas apresentarem possíveis soluções para o assunto.

A literatura atual apresenta IoT em uma estrutura de três camadas, camada de percepção, camada de rede e camada de aplicação. A camada de percepção, também chamada de camada de reconhecimento, reúne dados e informações relacionados ao meio físico. A camada de rede é a parte central dessa estrutura e também é conhecida como *wireless sensor network* (WSN). A camada de aplicação tem a função de coletar, processar e transmitir os dados. Alguns sistemas adotam mais uma camada ao utilizar um *middleware* como tecnologia de apoio a rede, essa camada seria, segundo [11] uma camada de processamento.

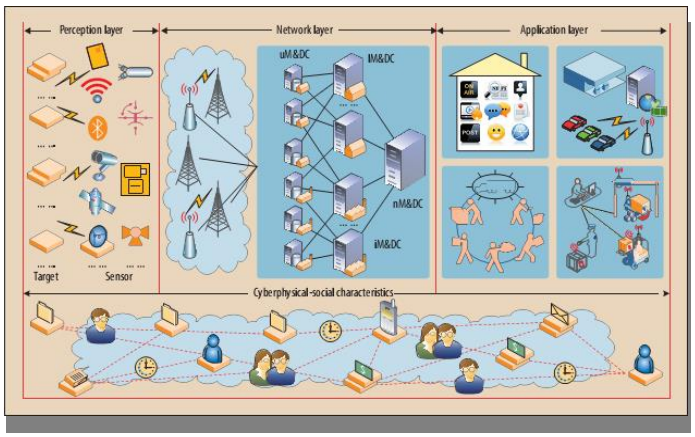

Fig. 1. Camadas de rede IoT [32].

Cada camada dessa estrutura apresenta suas próprias características relacionadas a problemas de segurança:

1) Camada de Percepção Problemas Conhecidos: A grande heterogeneidade dos nós de sensores e a baixa capacidade de armazenamento e processamento impedem a implementação de soluções de segurança mais complexas. Ref. [11] reporta algumas ameaças comuns a essa camada: captura de nós, nós falsos, *DoS*, *Timing Attack*, *Routing Threats*, *Replay Attack*, *Side Channel Attack*, problemas de autenticação em massa.

2) Camada de Rede Problemas Conhecidos: Embora as tecnologias tradicionais de segurança de rede já estejam bem estabelecidas e maduras, existem ainda possibilidades de ataques do tipo *man-in-the-middle* ou de negação de serviços DoS, voltadas a nós específicos da rede que podem comprometer seu funcionamento parcial ou como um todo. Há ainda questões relacionadas à compatibilidade entre o grande número de dispositivos ligados a rede o que dificulta a operabilidade entre eles.

3) Camada de Aplicação Problemas Conhecidos: Nessa camada os mecanismos de segurança podem gerar sobrecarga nas aplicações da rede sem fio. Garantir controle de acesso e identificar usuários nesse nível é trivial. Não obstante a segurança nessa camada é onerosa e mais complexa, permeada por questões como autenticação, permissão de acesso a dados, proteção e recuperação de dados, necessidade de lidar com um grande volume de dados, vulnerabilidades de software, etc.

III. PRIVACIDADE

De acordo com o Glossário de Segurança na Internet RFC 4949 privacidade pode ser definida como "o direito de uma entidade determinar o grau em que ela irá interagir com o seu ambiente, incluindo o grau que esta entidade está disposta a compartilhar suas informações pessoais com os outros." No que tange a privacidade na área da saúde muitos aspectos são relevantes e a natureza da informação é intrinsicamente mais crítica. Para tornar uma Rede de Sensores Biomédicos (BSN)

privada e garantir que os dados que nela trafegam não sejam expostos sem autorização, diversas são as propostas, a seguir as principais delas são analisadas.

Ref [12] sugere um modelo que usa técnicas de controle de fluxo de informação (IFC) representando o fluxo de dados como eventos que podem receber tags de acordo com suas propriedades de privacidade, permitindo que um computador confiável controle o acesso baseado em sensibilidade. Contudo considerando-se a baixa quantidade de recursos em cada nó de sensores e a quantidade de informação trafegando pela rede essa solução pode facilmente tornar-se inviável para uso em IoT. Isso devido ao custo computacional envolvido no processo de classificação da informação e a sobrecarga na rede esperada para esse procedimento.

Ref [13] apresenta um protocolo de autenticação mútua *key-changed protocol* para redes de sensores sem fio e RFID. Esse protocolo integra um gerador de números randômicos na *tag* e no *reader* e adota uma função HASH de mão única, técnicas de *key refresh* em tempo real, *key backup* entre outras. Segundo o autor as análises mostraram que o protocolo pode ser aplicado a sistemas IoT pelo seu baixo custo e prevenir com eficiência *DoS*, *Spoofing* e ataques de rastreamento de tags.

Em [14] aborda a fundo encriptação baseada em atributos (ABE) que habilita um controle de acesso de fina granularidade. Ele faz uma avaliação de desempenho do ABE focado em tempo de execução, sobrecarga de dados em rede, consumo de energia, e uso de CPU e memória. São testadas dois tipos principais de ABE, política de chaves KP-ABE e texto cifrado *CipherText* CP-ABE em diferentes classes de dispositivos móveis incluindo *laptops* e *smartphones*.

Na Ref [15] trata a questão da privacidade com algoritmos *Privacy Preserving Data Mining* (PPNM), minimizando sensivelmente a probabilidade de exposição dos dados pessoais. É proposto um esquema onde o usuário torna-se capaz de decidir que conteúdo compartilhar a partir de uma métrica de análise de dados inteligente. Os resultados descritos foram obtidos usando sensores de dados reais.

Em resumo podemos afirmar que em relação à privacidade ainda existem assuntos a serem explorados e uma ampla área de pesquisa a ser preenchida. Como vemos nos modelos [16-17-18] tratar completamente questões relacionadas à privacidade em sistemas IoT ainda é um desafio. Reconhecer as características de cada ambiente, dos dispositivos usados para compor a infraestrutura, bem como das pessoas que vão usar os sistemas pode ser a abordagem mais adequada a essa nova realidade.

IV. Protocolos de Comunicação

Como mencionado até aqui há muitos estudos relacionados à segurança em IoT sendo conduzidos neste momento.

Nesta seção será discutida a aplicabilidade e limitação dos protocolos de segurança baseados em IP e outros protocolos de segurança utilizados em WSN e WBAN, sua aplicação no contexto de IoT com ênfase em ambiente hospitalar eHealth.

A. Segurança Baseada em Chaves Criptográficas

O estudo apresentado aqui se caracteriza pela análise de entidades com restrições de recursos, nós de sensores RFID e demais dispositivos que podem possuir limitações ou serem nós computacionais plenos de capacidade. Estes são servidores externos com características de um roteador de borda sem restrições de recursos (6LBR), atuando como interconectores entre os nós de sensores e a rede externa.

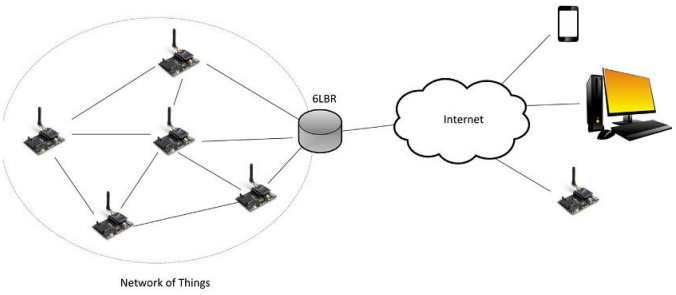

Fig. 2 Roteador de borda [20].

Alguns artigos analisados descrevem o uso de chaves de criptografia assimétrica, protocolos conhecidos e amplamente difundidos em aplicações de internet. Contudo esta abordagem apresenta alguns desafios ao ser aplicada no contexto de IoT, tais como o custo computacional envolvido na operação e o consumo de energia inadequado.

Outros pesquisadores propõem alternativas usando técnicas de criptografia simétrica que normalmente são compartilhadas por todos os nós envolvidos. Estas credenciais podem ser uma chave criptográfica ou alguns bytes carregados previamente nos próprios sensores.

Cada uma das soluções apresentadas adiante está empenhada em garantir o transporte seguro da informação na rede e possui suas próprias características, úteis ou inconvenientes, que serão discutidas a seguir:

Ref [19] fornece uma análise geral dos mecanismos existentes que utilizam chaves públicas e chaves pré-compartilhadas para nós de sensores no contexto de IoT. Analisa também a aplicabilidade na camada de ligação de *Key Management Systems* (KMS) cujo propósito principal é fornecer chaves compartilhadas a nós de sensores pertencentes à mesma rede WSN. Ele conclui que KMS podem ser viáveis como solução para nós de sensores funcionando em um modelo cliente-servidor, provendo um bom desempenho mesmo com as restrições existentes. Porém os critérios utilizados pelos autores levaram em consideração apenas a aplicação de chaves simétricas diferentemente de [20], onde ambas as chaves, simétricas e assimétricas, são amplamente exploradas.

No artigo [21] o autor propõe o uso adaptado através de mecanismos de compressão 6LoWPAN [22] de um *Datagram Transport Layer Security* (DTLS). Esse protocolo modificado reduz o tamanho dos cabeçalhos do protocolo padrão, proporcionando, segundo o autor, um ganho de desempenho em relação ao tamanho do pacote convencional. Há ainda uma redução no consumo de energia, tempo de processamento e a utilização de redes. Todas essas características são desejáveis

para tarefas sensíveis relacionadas à comunicação na camada de aplicação quando se fala em IoT no domínio eHealth.

Ref [23] apresenta uma abordagem semelhante em relação ao DTLS, contudo o *Handshake* é assistido por um roteador de borda 6LoWPAN (6LBR). O roteador de borda participa da comunicação de forma transparente entre nós de sensores e dispositivos conectados a internet. A proposta do autor provê segurança, integridade e autenticação para camada de transporte ao comunicar com dispositivos com restrição de recursos na camada de aplicação. Em outras palavras do ponto de vista do *Host* ele opera utilizando o protocolo DTLS convencional, por outro lado a comunicação realizada com a rede de sensores ocorre através de chaves pré-compartilhadas. Essa proposta carrega características inerentes ao Kerberos [24] ao passo que introduz uma abordagem nova para a comunicação entre essas duas camadas de dispositivos que compõe os ambientes de sistemas IoT.

B. Segurança Aplicada a Body Area Networks

Ref [25] reporta a implementação de um protocolo de segurança de alta frequência para *Wireless Body Area Network* (WBAN). Denominado MBStar suporta uma taxa de mensagens de 400 Hz para a rede de sensores. A camada física baseia-se na IEEE 802.15.4 com sequência direta de espalhamento de espectro. Em relação à segurança o autor sugere um esquema de encriptação que utiliza o par de chaves pública/privada e que não envolve nenhuma configuração humana na conexão dos dispositivos baseados em *Internet Exchange Key* (IKE), RFC 2409 [26].

Ref [27] faz uma profunda análise de diversos aspectos relacionados à WBANs e WSN, abordando questões como topologia, roteamento e frequências. No que tange a segurança o autor separa a comunicação em insegura, autenticada ou criptografada. Sugere para comunicação *unicast* chaves mestre pré-compartilhadas (MK) e *Pairwise Temporal Key* (PTK) chaves geradas para uso uma única vez por sessão. Para *multicast* sugere *Group Temporal Key* (GTK) a ser compartilhada com o grupo correspondente. Este estudo ainda levanta características inerentes a WBAN, disponibilidade, integridade, confidencialidade, etc. que devem ser observadas como requisitos para uma implantação segura dessa tecnologia.

Ref [28] detecta as falhas de segurança dos protocolos de criptografia relacionados à WBAN e as formas de ataque associadas a elas. Verifica os métodos de predição de falhas e investiga a implementação desses protocolos. Alguns ataques citados no artigo alertam para *know-key attack* onde chaves de segurança usadas anteriormente são armazenadas para uso malicioso posteriormente. *Impersonotion* em que atacantes tentam assumir a personalidade de membros legítimos da rede. *Relay* que basicamente grava mensagens e retransmite mais tarde. *Interleaving* onde falsas mensagens são injetadas na rede para danificar, alterar ou subverter os dados reais.

Ref [29] propõe um protocolo forte E-SAP para autenticação em larga escala em redes de sensores médicos utilizando criptografia simétrica para garantir confidencialidade na troca de mensagens. A proposta reivindica um baixo custo computacional e pouco consumo de energia para aplicações *healthcare*. Contudo no estudo apresentado por [30] esses resultados são questionados e o autor expõe vulnerabilidades encontradas na solução de segurança descrita anteriormente. Descreve ainda uma abordagem próxima aos 20% mais eficiente em relação ao consumo de energia comparada ao estudo anterior.

Ref. [33] apresenta um *framework* de detecção de intrusos (IDS) para IoT, nas palavras do autor: "com poderes IPv6 sobre dispositivos em redes pessoais de baixa potência (6LoWPAN)." O IDS proposto inclui um sistema de monitoramento e mecanismo de detecção. Um teste de penetração foi usado para avaliar o desempenho do *framework* IDS implementado, que preliminarmente revelou-se promissor como mecanismo de segurança para 6LoWPAN.

Até aqui este *survey* analisou e descreveu diferentes estudos relacionados à segurança e privacidade inerentes a redes de sensores aplicados a monitoramento e acompanhamento de saúde. A tabela II compara estes estudos apontando as características abordadas individualmente para cada um deles com o presente trabalho.

TABELA II. ASPECTOS RELEVANTES DOS ARTIGOS APRESENTADOS

	[11]	[12]	[13]	[14]	[15]	[19]	[20]	[21]	[23]	[25]	[27]	[28]	[29]	[30]	[33]	ESTE SURVEY
Segurança	x		x	x		x	x	x	x	x	x	x	x	x	x	x
Privacidade		x	x	x	x		x				x		x			x
Confidencialidade							x	x	x		x		x			x
Ameaças	x														x	x
Protocolos			x			x	x	x	x	x	x	x	x	x	x	x
Arquitetura	x	x							x	x	x		x		x	x
eHealth										x	x	x	x	x		x

V. CONCLUSÃO

Este artigo analisou múltiplas soluções de segurança para a implantação e desenvolvimento escalar de redes IoT em ambientes eHealth e redes de sensores sem fio (WSN). Este estudo perfez a estrutura de camadas de redes IoT e enumerou ameaças correspondentes a cada uma. Foram descritas características que dizem respeito à privacidade dos dados trafegando nestas redes. Por fim foram discutidos e comparados diferentes protocolos de segurança dispostos a garantir a integridade e confidencialidade da comunicação em redes de sensores e WBAN. A dinâmica dos sistemas descritos projeta um cenário de oportunidades nunca visto para comunicação. Para tanto é necessária uma abordagem específica que descreva os procedimentos a serem adotados desde as primeiras fases do processo. Não obstante uma visão que incorpore todas a diferentes características de IoT ainda é necessária. A heterogeneidade dos ambientes analisados requer ainda esforços a fim de garantir o grau adequado de segurança exigido para cada realidade.

REFERENCES

[1] M. Weiser, "The computer for the 21st century". in SIGMOBILE Mob. Comput. Commun. Rev.,1999, pp. 3–11.

[2] K. Ashton, "That 'Internet of Things' Thing", in RFID Journal, 22 June 2009. [Online]. Available: http://www.rfidjournal.com/ article/view/4986 Accessed on: Sep. 30, 2015

[3] Gartner inc., Forecast: The Internet of Things, Worldwide, 2013.

[4] K. Kang, Z. B. Pang, C. Wang, "Security and privacy mechanism for health internet of things," in Journal of China Universities of Posts and Telecommunications, 2013, pp.64–68.

[5] M. R. Abdmeziem, D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications," in Computers & Electrical Engineering, *44*, 2015, pp. 184–197.

[6] M. Li, W. Lou, K. Ren. "Data Secutiry and Privacy in Wireless Body Area Networks," in "IEEE Wireless Communications," 2010, pp. 51–58.

[7] S. M. R. Islam, D. Kwak, H. Kabir, "The Internet of Things for Health Care : A Comprehensive Survey," 2015 pp. 3.

[8] J. T. Kim, "Privacy and Security Issues for Healthcare System with Embedded RFID System on Internet of Things," 2014, pp. 109–112.

[9] Kumar, J. S. (2014). A Survey on Internet of Things : Security and Privacy Issues, *90*(11), 20–26.

[10] D. Wang, D. Evans, R. Krasinski, "Ieee 802.15.4J: Extend Ieee 802.15.4 Radio Into the Mban Spectrum, October 2012, pp.4–5.

[11] K. Zhao, L. Ge, "A survey on the internet of things security" Guangxi, China 2013, pp. 663–667. [9th International Conference on Computational Intelligence and Security]

[12] D. Evans, D. Eyers, "Efficient data tagging for managing privacy in the internet of things, in" IEEE Int. Conf. on Green Computing and Communications, GreenCom Conf. on Internet of Things, iThings and Conf. on Cyber, Physical and Social Computing, CPSCom, Besancon, France, 2012, pp. 244–248

[13] L.b. Peng, W.b. Ru-chuan, S. Xiao-yu, C. Long, "Privacy protection based on key-changed mutual authentication protocol in internet of things," in Commun. Comput. Inf. Sci. 418 CCIS 2014 345–355.

[14] X. Wang, J. Zhang, E. Schooler, M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT", [2014 IEEE International Conference on Communications], ICC 2014, Sydney, NSW, 2014, pp. 725–730

[15] A. Ukil, S. Bandyopadhyay, A. Pal, "Iot-privacy: To be private or not to be private", [Proceedings – IEEE INFOCOM], Toronto, ON, 2014, pp. 123–124

[16] S. Sicari, A. Rizzardi, C. Cappiello, A. Coen-Porisini, A NFP model for internet of things applications, in: Proc. of IEEE WiMob, Larnaca, Cyprus, 2014, pp. 164–171

[17] X. Huang, R. Fu, B. Chen, T. Zhang, and A. Roscoe, "User interactive internet of things privacy preserved access control," in 7th International Coriference for Internet Technology and Secured Transactions, ICITST 2012, London, United Kingdom, December 2012.

[18] Y. Wang and Q. Wen, "A privacy enhanced dns scheme for the internet of things," in IET International Conference on Communication Technology and Application, ICCTA 2011, Beijing, China, October 2011.

[19] R. Roman, C. Alcaraz, et al., "Key management systems for sensor networks in the context of the Internet of things", in Int. J. Comput. Electr. Eng. 2011 pp. 147–159

[20] K. T. Nguyen, M. Laurent, N. Oualha, "Survey on secure communication protocols for the Internet of Things." in *Ad Hoc Networks*, 2015 pp. 17–31.

[21] S. Raza, H. Shafagh, et al., Lithe: lightweight secure CoAPs for the Internet of things, IEEE Sens. J. 13 (10) (2013)

[22] J. Hui, P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, IETF, RFC 6282, 2011.

[23] J. Granjal, E. Monteiro, J. Silva, "End-to-end transport layer security for Internet-integrated sensing applications with ECC public-key authentication," in: IFIP Networking Conference, 2013.

[24] Neuman B, Ts'o T. Kerberos: an authentication service for computer networks. IEEE Communications Magazine, 1994, 32(9), pp. 33-38, DOI: 10.1109/35.312841

[25] X. Zhu, S. Han, P.-C. Huang, A. K. Mok, & D. Chen, "MBStar: A Real-time Communication Protocol for Wireless Body Area Networks." In 23rd Euromicro Conference on Real-Time Systems, 2011, pp. 57–66.

[26] "The internet key exchange (ike)," http://tools.ietf.org/html/rfc2409.

[27] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour. "Wireless Body Area Networks: A Survey." In Ieee Communications Surveys and Tutorials, 2014 pp. 1658–1686.

[28] J. Chaudhry, U. A. Qidwai, R. G. Rittenhouse, M. Lee. "Vulnerabilities and verification of cryptographic protocols and their future in Wireless Body Area Networks." in International Conference on Emerging Technologies, 2012 pp. 1–5.

[29] P. Kumar, S-G. Lee, H-J. Lee, "E-SAP: Efficient-Strong Authentication Protocol for Healthcare Applications Using Wireless Medical Sensor Networks," in Sensors (Basel, Switzerland). 2012 pp. 1625-1647.

[30] M. Sarvabhatla, C. S. Vorugunti, “An energy efficient mutual authentication scheme for secure data exchange in health-care applications using wireless body sensor network,” in 7th International Conference on Communication Systems and Networks (COMSNETS), 2015 pp. 1–6.

[31] Internet of Things Related Standards Available http://standards.ieee.org/innovate/iot/stds.html Accessed on: 30 Sep. 2015

[32] H. Ning, H. Liu, L. T. Yang, ”Cyberentity security in the internet of things,” in Computer, 2013. pp.46–53.

[33] P. Kasinathan, G. Costamagna, H. Khaleel, C. Pastrone, M. Spirito, “Demo: An ids Framework for Internet of Things Empowered by 6lowpan,” Berlin, Germany, 2013, pp.1337–1339.