Survey on the Emerging Security Challenges in the Internet of Things

Kaustav Ghosh
Computer Science and Engineering Department
Santa Clara University
CA 95050
Email:kghosh1@scu.edu

***Abstract*—The Internet of things (IoT) refers to an interconnection of a huge number of smart components and it includes various communications between these components in the network. Due to the ubiquitous and mobile nature of the components which form the IoT Network, IoT is often referred to as "anything, anyone, any service". This very advantage of the ubiquitous nature of IoT is a severe challenge for a secure IoT. Without a very strong technical and legal framework, the vulnerabilities in IoT will be exploited and this problem would definitely outweigh the advantages for which IoT was envisioned in the first place. To tackle this security issue in IoT, we need to first analyze the threats and security challenges in a IoT network. This survey paper helps you to understand the vulnerabilities and threats in the IoT framework. This paper also gives you an insight on how the present IP based security protocols cannot be used as is in the IoT framework and how researchers are presently working to modify the IP based security solutions for the IoT framework.**

I. Introduction

Internet of things (IoT) can be considered as a network of two or more things which can be connected and can communicate with each other through the internet. It can be as simple as a toaster embossing a sunny day or a rainy day on a bread depending upon the actual weather outside (by sensing the weather outside with the help of a temperature sensor). The Internet of Things definition can also be extended to the area of smart homes and smart cities where all the objects to which a person communicates with on a daily basis can itself communicate with each other and make the life of a the person much easier. For example your house door communicating with your car (with the help of a GPS on the car) and opening itself when the car enters the garage. The concept can also be extended to the healthcare domain where the body of a person can be monitored through smart objects connected to a remote cloud. So IoT can be considered as a network of smart objects to make the world a much more smarter place to live in.

IoT is a game-changing moment in our relationship with technology and personal data as we stand on the edge of a data explosion from interconnected devices. As with all new technologies, the IoT brings with it new challenges for businesses, regulators, consumers and in fact anyone who cares about the responsible use of data. With so many devices connected to each other through a network, there is always several risks involved ranging from physical stealing of these sensor elements on the IoT network to eavesdropping on the IoT network to extract personal information of the user and thus compromising the privacy of the user. There are various obstacles which hinder the ideal IoT vision and security is one of these key obstacles which requires significant attention. Due to the ubiquitous and constrained resource structure of the components in the IoT network, traditional internet security mechanisms are not enough for a secure IoT network. To create a strong foundation for technical and legal framework of a secure IoT, security experts must thoroughly understand the rising security and privacy challenges in the IoT framework and know how the existing web based security protocols can be modified to fit into this ubiquitous framework.

In this survey paper we first aim to present the various possible threats and vulnerabilities in the IoT framework. Then in the later half of the paper we describe the security challenges which security experts are presently facing and how they are working towards the goal of a secure IoT.

The rest of the survey paper is organized as follows. Section II gives an overview of the various threats and vulnerabilities in the IoT framework. In Section III we give a brief overview of the existing IP security protocols and finally in Section IV we discuss the security challenges in the IoT framework. Section V gives some suggested solutions for safeguarding the IoT framework from the security threats. Finally section VI includes some final remarks for the vision of a secure IoT.

II. Threats and Vulnerabilities

This section provides you with the various security threats and vulnerabilities in a typical IoT framework. We discuss about the security issues which could compromise the entire IoT network and we then classify these threats according to the TCP/IP stack layer they belong too. So this will give you a clear understanding as to which layer you need to focus on for a particular threat.

A. Privacy

Privacy is one of the most important concerns when it comes to security related to IoT. The ubiquitous nature of the components which form the IoT infrastructure generates a tremendous amount of data which can be available to a hacker if the hacker intrudes into this infrastructure. Majority of this data would be generated by a user and if the hacker can gather this data, there would potentially be a breach in the

privacy of the user. This information can thereafter be sold by the hacker to some other company for money. This privacy and data protection security breach can lead to heavy fines which the IoT service providers would have to pay. Hence an extra attention should always be paid to the security of the data center infrastructure that stores the data gathered by the IoT components. The additional cost to prevent this kind of security breach is much lesser than the cost which the service provider would have to pay as penalty if the privacy of the users is compromised.

As mentioned in [1], the the privacy issue can be tackled in three different ways.

1) Privacy by Design wherein a user would use the tools they need to manage their own data.
2) Transparency wherein users know the entities which are managing their data and how their personal data is being used. The IoT service providers should also be part of this process by having various license agreements to support this process.
3) Data Management wherein there needs to be strict policies which needs to be followed to manage various kinds of data. These policies should align with legislation on data protection.

By following these principles and a strong data-management framework as mentioned above, policymakers should develop policies that address privacy and security concerns for IoT while also ensuring that the ultimate vision of IoT is not killed.

Due to the above mentioned privacy challenges of a user, the regulators at the US Federal Trade Commission and various other government organizations of different countries are looking at privacy and security issues related to IoT. Potential criminal activity must be addressed with this technology boom. This protection of the data in the IoT infrastructure is everyone's responsibility, starting from end users to the service providers. Industry collaboration and not competition would help in deciding common standards, be it security and privacy standards or network standards. Mutual understanding and collaboration is extremely essential to support a broader IoT ecosystem and perform secure operations in this insecure infrastructure.

B. Substitution of Components

While deploying components in the IoT network there might be a possibility wherein a high quality component may be replaced by a low quality component without it being detected for it's lower level of quality. The reason behind this may be cost savings. This may degrade the performance of the IoT network as a whole and can be an entry point into the system for further threats.

C. Eavesdropping

As mentioned in [2] eavesdropping during the deployment of a component in the IoT network can be a major threat due to the the exchange of cryptographic keys, security parameters and other security configuration settings during the bootstrap process. After obtaining certain security parameters the hacker may be able to communicate with various other components on the network and thereby compromising the security of the communication channel. This security of the communication channel can also be compromised when two components in the network are communicating and if the channel is not sufficiently protected. To prevent this there needs to be a continuous renewal/update on the session keys which is used for communication between the components.

H. Jeon, J. Choi, S. McLaughlin, and J. Ha in [3] provide an elegant encryption solution to the eavesdropping problem in a wireless sensor network in which the authors have used simple and efficient physical layer security concepts to provide confidentiality to the data in a wireless sensor network (WSN). A similar solution can also be adopted for a IoT network to prevent it from the eavesdropping threat.

D. Denial Of Service Attack (Dos Attacks)

The components which make up the IoT network typically have constrained resources like limited memory and limited power for its operations. Any activity that reduces, eliminates or disrupts the network's communication is categorized as a DoS attack. Device availability is one of the key features of the IoT infrastructure. A DoS attack can jam or flood the entire communication channel of the IoT network thus tearing down the network. This compromises the network availability and in turn makes several devices on the network unavailable. Attackers can take advantage of these constrained components in the IoT infrastructure by continuously sending requests to these components and ultimately exhausting the battery life of the component and thus preventing it from functioning any further.

Since IP was considered impractical for low power devices like the one's used in the IoT network, IoT devices typically work over low power wireless area networks-6LoWPAN [4]. P. Kasinathan, C. Pastrone, M. Spirito, and M. Vinkovitsv in [5] provide a DoS detection architecture for 6LowPAN operating over the IoT devices. The authors integrate an intrusion detection system with a network framework developed within EU FP7 project ebbits.

E. Stealing of physical hardware

There are various hardware components like sensors which are deployed in the environment as a part of the IoT network. These components are usually unprotected and can be easily captured by an intruder. Such an intruder can extract various security parameters from the device . As mentioned in [2], if the group key is compromised using these security parameters, the entire group network is compromised. Compromising a unique key specific to that device is better than compromising the entire network using a group key. Thus one has to be very careful while communicating these group keys over a channel since compromising a group key may result in compromising of the entire group network.

F. Sinkhole attack

The IPv6 Routing Protocol for low power and lossy networks, commonly known as RPL [4] is a standard routing

Table I
DISTRIBUTION OF THREATS/VULNERABILITIES ACCORDING TO TCP/IP LAYERS

TCP/IP Layer	Threats/Vulnerabilities.
Application Layer	Extraction of Security Parameters, Firmware Updates.
Transport Layer	Eavesdropping and Man-in-the-middle attack.
Network Layer	DoS attack, Routing attack, Eavesdropping and Man-in-the-middle attack .
Physical Layer	DoS attack .

protocol for IoT networks and is used in a 6LoWPAN network. Sinkhole Attack is one of the routing attacks in a 6LoWPAN network. As mentioned in [6], in a sinkhole attack a malicious node lures all the traffic around it in the network by advertising an attractive path. Sinkhole attacks like the one described in Fig. 1., are difficult to counter because routing information supplied by a node is difficult to verify.

T. V. Linus Wallgren and Shahid Raza in [7] do an experimental study to see if the RPL protocol can counter against the Sinkhole attack or try reducing its impact.

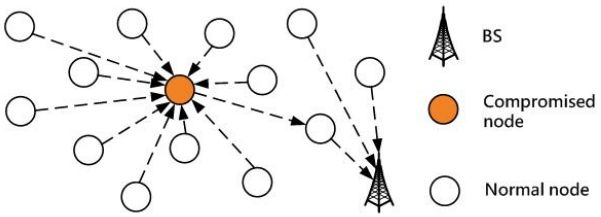

Figure 1. Depicts a simple Sinkhole attack where the orange node is the malicious node

G. Selective Forwarding

As mentioned in [8], in this sort of a routing attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There might arise a case in the selective forwarding attack wherein the malicious node selectively drops the packets coming from a particular node or a group of nodes. This attack as we can see from Fig. 2., can prove to be disastrous for the network if coupled with attacks like the sinkhole attack discussed in the above section.

The author in [7] provides a solution against the selective forwarding attacks wherein the author suggests to create disjoint paths between source and destination nodes. Although this solution is very difficult to implement in huge networks since creating disjoint paths for the entire network is quite hard but this can be easily implemented in small networks. One elegant solution can also be to not let the attacker know which type of traffic he/she is receiving which would force the attacker to either forward all or none of the traffic.

TABLE I depicts the threats corresponding to each of the layers in TCP/IP stack.

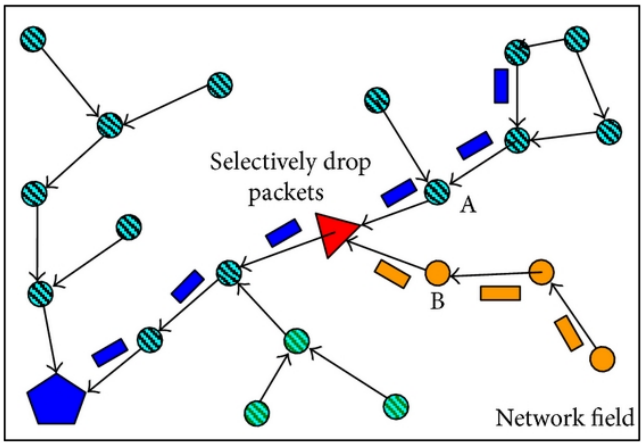

Figure 2. Depicts a simple case of Selective Forwarding where the Red Node is dropping packets which it is receiving from node B

III. IP BASED SECURITY CHALLENGES

Firstly we need to have a brief overview of the existing Internet based protocols which we will refer to understand the security challenges in the IoT framework.

A. IP based Security Solutions

One of the weakest points of the original Internet Protocol is that is lacks basic security mechanisms like authenticity and privacy of data of the user in the network. With the growth of the Internet and millions of people using it, security mechanisms were needed for IP. To facilitate this need, IP Security (IPsec) protocol was developed. While a wide range of specialized as well as general-purpose key exchange and security solutions already exist for the Internet domain, we discuss a number of protocols and procedures that have been recently discussed in the context of the above working groups. The considered protocols are IKEv2/IPsec [9], TLS/SSL [10], DTLS [11], HIP [12] [13], PANA [14], and EAP [15] in this Internet-Draft.

The Internet Key Exchange (IKEv2)/IPsec and the Host Identity protocol (HIP) reside at or above the network layer in the OSI model. IKEv2 or IKE is a part of the IPsec protocol suite which helps to set up a security association. HIP on the other hand is a host identification technology for use on IP. HIP creates the Host Identity (HI) based on a public key security infrastructure. Both these above mentioned protocols are able to perform an authenticated key exchange and set up IPsec transformations for secure payload delivery. Currently, there are also ongoing efforts to create a HIP variant coined Diet HIP [12] that takes lossy low-power networks into account at the authentication and key exchange level.

Transport Layer Security (TLS) and its datagram oriented variant DTLS secure transport layer communications and prevent attacks like eavesdropping and tampering on the network. TLS provides security for the TCP layer in a IP network and requires a reliable transport. TLS uses asymmetric cryptog-

raphy to authenticate the user with another user to exchange a symmetric key. Although TLS protects the transport layer but it is initialized at the session layer and it works at the presentation layer of the TCP/IP network model. DTLS on the other hand secures and uses datagram-oriented protocols such as UDP. Both protocols are intentionally kept similar and share the same ideology and cipher suites.

The Extensible Authentication Protocol (EAP) is an authentication framework supporting multiple authentication methods. It is widely used in wireless networks like IEEE 802.11 (Wifi). The WPA and WPA2 standards have adopted more than hundred EAP types as official authentication mechanisms. It is used to transport keying material and parameters generated by EAP methods [15]. EAP runs directly over the data link layer and, thus does not require the deployment of IP.

IV. Security Challenges in the Internet of Things framework

In this section we discuss about the different security challenges in the IoT framework and also discuss how the existing internet security protocols interoperate with this IoT framework and what are it's limitation. Majority of the security challenges are created due to the resource constraint features of the devices on the IoT network. In the section below we'll discuss about the security threats which the IoT infrastructure is facing due to it's device's resource constraints and we'll also discuss about the rising security challenges related to cryptography algorithm processing, authentication and also identity management which is one of the major challenges in the IoT domain.

A. Security Challenges due to Resource Constraints

Interoperating resource constrained devices on a network with the Internet is a very big challenge because of the heterogeneity of both the networks. The IoT infrastructure has resource constrained components as a part of its network and these components rely on low bandwidth channel and have limited memory, CPU and power resources. These characteristics of the IoT network affects the security protocol designs and limits the use of the existing Internet based security protocols. For example, as mentioned in [2], IEEE 802.15.4 (used in networks having resource constraint devices) supports 127-byte sized packets at the physical layer which may result in fragmentation of larger packets of security protocols. This may open new attack vectors for DoS attacks, which is specially dangerous if the fragmentation is caused by large key exchange messages of security protocols.

Another issue is the usage of public key cryptography in the IoT network. Due to the limitations on memory and power resources in the IoT network components, the use of such crypto primitives is not recommended. In view of these limitations, there has been attempts to reduce the cost involved in public key based key exchanges. Diet HIP takes the reduction of this cost to a next level by focusing on implementing cryptographic functions on IEEE 802.15.4 compliant device's hardware. As mentioned in [2], Diet HIP does not require cryptographic hash functions but uses a CMAC [16] based mechanism, which can directly use the AES hardware available in standard sensor platforms.

Standard and trusted suite of cryptographic algorithms like the AES, RSA and Diffie-Hellman key exchange algorithms were designed with the assumption that significant system resources like memory and processor speed would be available. So the use of these standard cryptographic security algorithms in these resource constrained devices on the IoT network is unclear and requires further analysis to make sure that they don't drain out the resources of the IoT devices and make it unavailable.

B. End to End Security Issue

The Core of the IoT network has to ideally run on a de facto constrained IP network-6LoWPAN [4]. This is analogous to the IPv6 internet protocol. Similarly analogous to to the HTTP protocol which works at the application layer, there is a protocol for the IoT framework which is the Constrained Application Protocol (CoAP) [17] which runs over UDP and enables efficient communication of things at the application layer.

Both CoAP and 6LoWPAN are steps towards reducing the difference between existing internet protocols and IoT but still there are certain major differences between the both due to performance reasons. These differences can be bridged easily at gateways but it can be a major obstacle if there is end-end security measures deployed between the IoT devices and the hosts on the Internet since these end-end security measures don't allow the gateways to decrypt the messages and modify them according to the network since that would compromise the end to end security. There are various solutions to tackle this solution which are mentioned in detail in [2].

As mentioned in [18], the implementation of end to end security protocols in resource constrained IoT networks is a big challenge due to the limited computational power and memory of the devices in the IoT network. These constraints make the complicated end to end security protocols not useful for the IoT infrastructure. The authors in [18] provide a modification of the end to end security protocols like IPsec and DTLS to make them work efficiently in the IoT network.

C. Distributed vs Centralized Architecture Security Issues

Currently most of the IoT architectures are centralized for example the ZigBee standard is completely centralized and depends on a central server called the trust center. In a centralized architecture there is a central management of devices and the cryptographic keys are stored in the a central server too. This provides for a single point of failure which is a severe drawback . Also without a well managed security infrastructure creating ad hoc security domains with certain new nodes is not possible. Decentralized architectures instead allow to create ad hoc domains of new nodes which do not require a well established security infrastructure and can act in a stand-alone way. This would reduce the single point of

failure issue for the entire network which exists in a centralized architecture.

D. Identity Management and Key distribution Issue

As we connect various things to the Internet we also need ways of ensuring they are what they claim to be. This creates an interesting challenge, that is how to manage the identities of all these connected devices we are in the process of communicating, in all their scenarios, shapes and sizes. Identity management was never easy but it looks set to become even harder because it is estimated that by 2020, over 20 billion devices with be connected to the internet (over two times the human population on earth at that time).

During the bootstrapping process, security related information is passed on to the components of the IoT network which enables a secure communication channel between these devices. How this security related information is passed is different in distributed and centralized IoT architectures. If we do not consider the resource limitations of things, certificates and certificate chains can be employed to securely communicate capabilities in such a decentralized scenario. As mentioned in the previous section too, Diet HIP doesn't require a device to implement cryptographic hashes to limit energy loss due to calculations of hashes.

As mentioned in [2], in a centralized architecture, preconfigured keys or certificates held by a thing can be used for the distribution of operational keys in a given security domain. A current proposal [19] refers to the use of PANA for the transport of EAP messages between the PANA client (the joining thing) and the PANA Authentication Agent (PAA). EAP is thereby used to authenticate the identity of the joining thing.

Considering the limited resources of the IoT devices there needs to be a provision for a lightweight Public Key Infrastructure where the IoT devices can use the traditional or IoT specific symmetric encryption for data exchange.

V. Security Solutions for the IoT framework

As discussed in the previous sections, there exists a huge array of threats and security challenges which the IoT infrastructure presently faces, thus there is no single solution which makes the IoT network secure. But after analyzing the threats and various security challenges we can narrow down upon certain security solutions which can be applied to the IoT network and we discuss these solutions in this section. This section takes you through the steps to be taken right from the initial design to the deployment phase of a IoT network to make the infrastructure secure.

A. Booting Securely

When switching on a device in the IoT, the authenticity of the device is checked using traditional cryptography tools or customized low power consuming cryptography algorithms. As mentioned in [20] authenticating securely during the booting process using digital signatures and cryptographic key exchanges is very essential and compromising this information would lead to compromising the security of the entire device or possibly the entire network. Although there is a secure connection established, but the device still needs security from the run time threats in the network. For example-routing attacks like the Sinkhole and the Selective forwarding attacks can affect the network at anytime during the lifecycle of the network. Olaf Bergmann, Stefanie Gerdes, Silke Schafer, Florian Junge and Carsten Bormann discuss in [20] about the importance of securely configuring a IoT network and it provides us with an elegant three phase protocol to securely bootstrap the nodes in a Wireless Sensor network based on IPv6 and CoAP which is very much similar to the IoT network.

B. Resource Control

For different components of a device in the IoT, various access controls should be applied for accessing resources of the device. This would ensure that if one component of a device is compromised, then other resources on which the component doesn't depend wont be compromised. This decoupling of resources as mentioned in [21] by limiting system privileges for different components of a device would be really helpful in a ubiquitous type network like the IoT. The authentication and access control issue is dealt in great detail in [21] where the authors analyze the existing access control methods and then design a novel solution for IoT infrastructure using the already existing authentication and access control mechanisms.

C. Firewall Protection

Just like Intranet, a IoT network would also need a firewall to regulate traffic that is destined to itself and its corresponding network. As pointed out in [22], this would greatly help in filtering messages according to the protocol message header since each embedded device in a IoT network can use a different protocol for communication. So this helps in reducing the load on the devices to compute the decision whether the received message belongs to itself or not. The firewall computes that decision for the components and a device gets messages only directed to itself. All this in turn helps in reducing attacks or spreading of attacks to different types of nodes handling different packets in the network. So if one node in the network is affected due to a malicious message/packet some other node handling a different packet type may not be affected because of it.

D. Software Updates

Once a device is deployed in the field there needs to be regular updates on them. Service providers will roll out the update patches and the devices need to update their software in a way that does not compromise or expose the device to various threats in the IoT environment. So there needs to be a provision in the software updates and patches wherein the security of the device is not at all compromised. Also there needs to be way by which we can optimize the energy or resource consumptions for updating these patches on the resource constrained devices in the IoT network. Apurva

Mohan in [23] gives a very interesting use case of Personal Medical Devices (PMD) attached to a patients body for health monitoring wherein the author describes the importance of software updates in a resource constraint device like a PMD and how a security breach on a device like that can even kill a person.

VI. Conclusion

The Internet Of Things is already more than just a thought and has already started to gather momentum making life of it's users simpler. By complying with the security requirements, IoT can be considered as a complete paradigm which will soon be at it's peak. There are still open problem areas such as cryptographic mechanisms, interoperability of Internet protocols, data, identity management, privacy of the user and de-facto architectures. There needs to be future research work which would carefully consider the balance of governance and legal framework with innovation. Finally security cannot be considered just an add on to the IoT device but rather should be considered as an integral part of the IoT infrastructure.

References

[1] R. Roman and J. Najera, Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, Sept 2011.

[2] S. K. R. H. R. S. Garcia-Morchon, S Kumar, "Security Considerations in the IP-based Internet of Things," Working Draft, IETF Secretariat, Internet-Draft draft-garcia-core-security-O.txt, Sep. 2011.

[3] H. Jeon, J. Choi, S. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," in *Information Forensics and Security (WIFS), 2011 IEEE International Workshop on*, Nov 2011, pp. 1–6.

[4] A. B. T. Winter, P. Thubert, "RPL: IPv6 routing protocol for low-power and lossynetworks," Internet Requests for Comments, RFC Editor, RFC 4919, March 2012. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4919.txt

[5] P. Kasinathan, C. Pastrone, M. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*, Oct 2013, pp. 600–607.

[6] V. C. Vinay Soni, Pratik Modi, "Detecting sinkhole attack in wireless sensor network," vol. 2. IJAEIM, February 2013.

[7] T. V. Linus Wallgren, Shahid Raza, "Article: Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 2013, no. 794326, p. 11, February 2013.

[8] M. Y. A. Q. A.-I. Wazir Zada Khan, Yang Xiang, "Article: Comprehensive study of selective forwarding attack in wireless sensor networks," *Computer Network and Information Security*, vol. 1, no. 17, pp. 1–10, February 2011.

[9] E. Kaufman, "Internet Key Exchange (IKEv2) Protocol," Internet Requests for Comments, RFC Editor, RFC 4306, Dec 2005. [Online]. Available: http://www.rfc-editor.org/rfc/rfc4306.txt

[10] R. Dierks, "The Transport Layer Security(TLS) Protocol Version 1.2," Internet Requests for Comments, RFC Editor, RFC 5246, Aug 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5246.txt

[11] Phelan, "Datagram Transport Layer Security (DT SLS) over the Datagram Congestion Control Protocol (DCCP)," Internet Requests for Comments, RFC Editor, RFC 5238, May 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5238.txt

[12] J. P. E. Moskowitz R., Nikander P., "Host Identity Protocol," Internet Requests for Comments, RFC Editor, RFC 5201, May 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5201.txt

[13] J. H. Moskowitz, Heer, "Host Identity Protocol Version 2," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-hip-rfc5201-bis-13, Sep. 2013.

[14] E. B. P. H. T. A. Y. D. Forsberg, Y. Ohba, "Protocol for Carrying Authentication for Network Access (PANA)," Internet Requests for Comments, RFC Editor, RFC 5191, May 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5191.txt

[15] V. J. C. J. H. E. Aboba B., Blunk L., "Extensible Authentication Protocol (EAP)," Internet Requests for Comments, RFC Editor, RFC 3748, May 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3748.txt

[16] M. J. Dworkin, "Sp 800-38b.nist specification publication," Gaithersburg, MD, United States, Tech. Rep., 2005.

[17] C. B. Z Shelby, K Hartke, "Constrained Application Protocol (CoAP)," Working Draft, IETF Secretariat, Internet-Draft draft-ietf-core-coap-18, 2013.

[18] A. D. Rubertis, L. Mainetti, V. Mighali, L. Patrono, I. Sergi, M. L. Stefanizzi, and S. Pascali, "Performance evaluation of end-to-end security protocols in an internet of things," in *2013 21st International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013), Split-Primosten, Croatia, September 18-20, 2013*, 2013, pp. 1–6.

[19] O. C. C. O'Flynn, Sarikaya, "Security Bootstrapping of Resource-Constrained Devices," Working Draft, IETF Secretariat, Internet-Draft draft-oflynn-core-bootstrapping-03, Nov. 2010.

[20] O. Bergmann, S. Gerdes, S. Schafer, F. Junge, and C. Bormann, "Secure bootstrapping of nodes in a coap network," in *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*, April 2012, pp. 220–225.

[21] J. Liu, Y. Xiao, and C. Chen, "Authentication and access control in the internet of things," in *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, June 2012, pp. 588–592.

[22] I. Ishaq, J. Hoebeke, I. Moerman, and P. Demeester, "Internet of things virtual networks: Bringing network virtualization to resource-constrained devices," in *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on*, Nov 2012, pp. 293–300.

[23] A. Mohan, "Cyber security for personal medical devices internet of things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, May 2014, pp. 372–374.