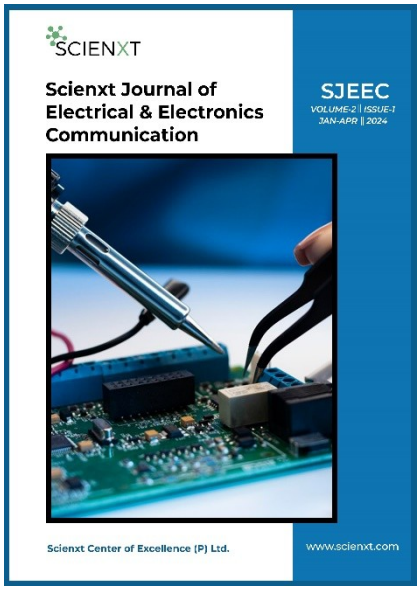

Scienxt Journal of Electrical & Electronics Communication
Volume-2 || Issue-1 || Jan-Apr || Year-2024 || pp. 1-15

A Literature survey of IOT techniques

[*1]Nehul Mathur, [2]Priyanka Valmiki, [3]Upendra Kumar

[*1]Assistant Professor, Department of Electronics& Communication Engineering, Bhopal Institute of Technology, Bhopal (M.P) India

[2,3]Student, Department of Electronics& Communication Engineering, Bhopal Institute of Technology, Bhopal (M.P) India

**Corresponding Author: Nehul Mathur*
Email: bitbhopal29@gmail.com

Abstract:

The Internet of Things (IoT) has a vision of a future where Internet users, computer systems, and everyday objects with sensing and actuation capabilities cooperate with the unprecedented convenience and economic benefits. As with the current architecture of the Internet, IP-based communications protocols will play a key role in enabling ubiquitous connectivity of devices in the context of IoT applications. These communication technologies are developed in accordance with the constraints of platforms may be used by applications to the detection of IoT, forming a communication stack capable of providing the required power-efficiency, reliability and connectivity Internet. Security will be a factor fundamental to most applications of IoT, mechanisms must also be designed to protect communications made possible by these technologies. This study analyzes existing protocols and mechanisms to secure communications in the IoT, as well as issues of open research. We analyze how existing approaches ensure that the basic safety requirements and protect communications on the IoT and the open challenges and strategies for future research in the field. This is, as far as our knowledge goes, the first survey with those goals.

Keywords:

IoT, Bluetooth, ZigBee, DTLS, RFID, IEEE 802.15.4 standard

1. Introduction:

The Internet of Things (IoT) is an important topic in the technology industry, politics, and engineering circles and became headline news in the trade press and popular media. This technology is incorporated into a wide range of network products, systems and sensors that take advantage of advances in computing power, electronics miniaturization and interconnection of networks to offer new features not previously possible. A conference abundance, reports and press articles discuss and debate the potential impact of "IoT revolution" -to new market opportunities and business models to concerns about security, privacy and technical interoperability.

The large-scale implementation of IoT devices promises to transform many aspects of how we live. For consumers, the new IoT products such as Internet-enabled devices, home automation components, and energy management systems to guide us towards a vision of "smart home", providing greater efficiency and security Energy. Other personal devices IoT devices as fitness and portable health monitoring and medical device license network are transforming the way health services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, thereby improving levels of independence and quality of life at a reasonable cost. IoT systems as networked vehicles, intelligent transport systems and sensors embedded in roads and bridges bring us closer to the idea of "smart cities", which help to reduce congestion and energy consumption. The IoT technology offers the possibility of transforming agriculture, industry and the production and distribution of energy by increasing the availability of information along the production value chain using networked sensors. However, the IoT raises many issues and challenges that need to be considered and addressed if the potential benefits to be realized.

Some observers see the IoT as fully interconnected world revolutionary "smart" progress, efficiency, and the ability, with the ability to add billions of value to the industry and the global economy. Others warn that the IoT represents a darker world of surveillance, privacy and security breaches, and consumer lock-in. Attention-grabbing titles on piracy of Internet-connected cars, concerns arising from supervisory voice recognition features in "smart" TVs, and fears of privacy deriving from the IoT data from potential abuse captured the public attention. This debate "promise vs risk" and a flood of information that the popular media and marketing can make IoT a complex subject to understand.

Basically, the Internet Society cares for the IoT, it represents an aspect increasingly the way people and institutions are likely to interact with the Internet in their personal, social and economic. If even modest projections are correct, explosion IoT applications could pose a

fundamental change in the way users interact with and affected by the Internet, which raises new questions and the different dimensions of the existing challenges through the user / consumer concerns, technology, politics and law. IoT will also probably different consequences in different economies and regions, bringing a diverse set of opportunities and challenges worldwide.

2. Iot technologies:

The Internet of Things was first inspired by members of the RFID community, who have raised the possibility of discovering information about a tagged object by browsing an Internet address or a database entry corresponding to an RFID particular technology or Near Field Communication. In the research paper "The research and application of intelligent home-based component technologies and Internet of Things", the key technologies of IoT are included RFID, sensor technology, nano technology and the technology embedded intelligence. Among them, the RFID is the basis and core networking building the Internet of Things. The Internet of Things (IoT) allowed users to make physical objects in the field the cyber world. This was made possible by various marking technologies such as WSN, RFID and 2D bar codes that enabled physical objects to be identified and sent on the Internet.

2.1. Radio Frequency Identification (RFID):

Radio Frequency Identification (RFID) is a system that transmits the identity of an object or a person using wireless radio waves in the form of a serial number. First use of RFID arrived in WW2 in Brittan and is used to identify Friend or Foe in 1948. RFID is later founded the Auto-ID Center at MIT in 1999. RFID technology plays a role IOT important to resolve objects identification problems that surround us in a profitable manner.

2.2. Internet protocol (IP):

Internet Protocol (IP) is the primary network protocol used on the Internet, developed in the 1970s is the main IP communication protocol in the Internet protocol suite for relaying datagrams across network boundaries. Both versions of Internet protocol (IP) are in use: IPv4 and IPv6. Each version defines an IP address. Because of its prevalence, the generic term IP address is still generally refers to the addresses defined by IPv4. There are five classes of available IP ranges in IPv4: Class A, Class B, Class C, Class D and Class E, while only A, B and C are commonly used. The current protocol provides 4.3 billion addresses IPv4 while

IPv6 will significantly increase the availability to 85.000 trillion addresses. IPv6 is the Internet protocol of the 21st century. It supports around 2128 addresses.

2.3. Electronic product code (EPC):

Electronic Product Code (EPC) is a 64 code bits or 98 bits recorded electronically on an RFID tag and for designing an improvement in the EPC system barcodes. EPC code can store information about the type of EPC unique serial number of the product, its specifications, manufacturer information etc. EPC was developed by the Auto-ID Center at MIT in 1999. EPCglobal organization that is responsible for the standardization of electronic product code (EPC) technology, created EPCglobal RFID network for information sharing.

2.4. Barcode:

Barcode is just a different way of encoding numbers and letters by using a combination of bars and spaces of varying width. The bar codes are readable by optical engine labels attached to elements that store information related to the element. Recently, the QR code system has become popular outside of the automotive industry due to its fast readability and greater storage capacity compared to the standard. There are 3 types of digital codes Alpha bars, digital and 2 dimensions. Barcodes are designed to be machine readable. Usually, they are read by laser scanners, they can also be read using one of the cameras.

2.5. Wireless fidelity (Wi-Fi):

Wireless Fidelity (Wi-Fi) is a network technology that allows computers and other devices to communicate over a wireless signal. Today, there are nearly ubiquitous Wi-Fi that provides the high speed wireless LAN (WLAN) connectivity to millions of offices, homes and public places such as hotels, cafes and airports. The integration of Wi-Fi in laptops, handhelds and consumer electronics (CE) devices has accelerated the adoption of Wi-Fi to the point where it is almost a fault in these devices. Technology contains any type of product support any WLAN IEEE 802.11 with dual-band, 802.11a, 802.11b, 802.11g and 802.11n. Today, entire cities become Wi-Fi corridors through wireless access points.

2.6. Bluetooth:

Bluetooth wireless technology is a low-cost radio technology for short-range eliminates the need for professionals. Prietary cabling between devices such as laptops, handheld computers, PDAs, cameras and printers and effective range of 10-100 meters. And generally communicate at less than 1 Mbps and Bluetooth specification uses the IEEE 802.15.1

standard of.

2.7. ZigBee:

ZigBee is a protocol developed to improve the characteristics of wireless sensor networks. ZigBee technology is created by the ZigBee Alliance, which was founded in 2001. Characteristics of ZigBee are low cost, low data rate, relatively short transmission distance, scalability, reliability, flexible protocol design. It is a supply network protocol without low wire based on the IEEE 802.15.4 standard. ZigBee has a range of about 100 meters and a bandwidth of 250 kbps.

2.8. Wireless sensor networks (WSN):

A WSN is a wireless network consisting of autonomous devices distributed in space using sensors to monitor in collaboration physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants at different locations. Formed by hundreds or thousands of granules which communicate with each other and transmit data along one to another. A wireless sensor network is an important element in the IoT paradigm. Sensor nodes may have no global ID because of the large amount of overhead and large number of sensors.

3. Main technical issues:

Five key areas of IoT issue are examined to explore some of the most pressing challenges and issues related to technology. These include security; privacy; interoperability and standards; legal, regulatory, and rights; and the emerging economy and development issues. These problems can be described as follows:

1. Security
2. Privacy
3. Interoperability / Standards
4. Legal, Regulatory and Rights
5. Emerging Economy and Development Issues

3.1. Security:

While security considerations are not new in the context of information technology,

attributes many implementations IoT present new unique challenges in terms of security. To meet these challenges and ensure security in the IoT products and services should be a key priority. Users need to trust that the IoT devices and related data services are protected from the vulnerabilities, especially as the technology becomes more widespread and integrated into our daily lives. IoT devices and poorly secured services can serve as potential entry points for cyber-attacks and expose user data theft by letting the flow poorly protected data.

The interconnected nature of IoT devices means that each poorly secured device that is connected online potentially affect the security and resilience of the Internet globally. This challenge is amplified by other considerations such as mass deployment across homogeneous IoT devices, the ability of some devices to connect automatically to other devices, and the likelihood of fielding these devices in unsecure environments.

The variety of new Wi-Fi enabled internet devices will create a data stream for companies to collect, aggregate, process and analyze. While certainly organizations identify new business opportunities based on these data, new risks are also emerging.

3.2. Privacy:

The full potential of the Internet of things depends on the strategies that respect the choice of the privacy of individuals across a wide range of expectations. The data flow and user specificity offered by IoT devices can unlock an incredible and unique value to users IoT, but concerns about privacy and the potential harm could retain the full adoption of the Internet of Things . This means that the rights of privacy and respect expectations of privacy of the user are an integral part of ensuring user confidence and trust in the Internet, connected devices, and related services.

Indeed, the Internet of Things is redefining the debate on privacy issues, many implementations can dramatically change the ways personal data is collected, analyzed, used and protected. For example, the IoT amplifies concerns about the possibility of increased surveillance and monitoring, trouble to be able to pull some data collection, and the strength of aggregation of data flows IoT to paint detailed digital portraits users. While these are significant challenges, they are not insurmountable. To realize the opportunities, strategies must be developed to respect individual choices for privacy in a wide range of expectations, while encouraging innovation in new technologies and services.

3.3. Interoperability / standards:

A fragmented environment of IoT proprietary technical implementations will inhibit value to

users and industry. While full interoperability between products and services are not always possible or necessary, buyers may be reluctant to buy goods and services IoT if inflexibility of integration, high complexity of ownership, and concern vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for network resources, they connect to the Internet and wider. Appropriate standards, reference models and best practices will also help curb the proliferation of devices that can act so disturbed the internet.

3.4. Legal, regulatory and rights:

The use of IoT devices raises many new regulatory and legal issues and amplifies the legal issues around the existing Internet. The questions are broad in scope and pace of change in IoT technology often exceeds the capacity of the associated political, legal, and regulatory structures to fit.

Although legal and regulatory challenges are large and complex in scope, the adoption of the guiding principles of the Internet Society to promote a user's ability to connect, speak, innovate, share, select, and trust are essential considerations in changing laws and regulations that allow rights of IoT user.

3.5. Emerging economy and development issues:

The Internet of things is very promising to provide emerging social and economic benefits and development. This includes areas such as sustainable agriculture, water quality and use, health, industrialization and environmental management, among others. As such, the IoT is promising as a tool in achieving the United Nations sustainable development goals.

The scope of IoT challenges will not be the preserve of industrialized countries. Developing regions will also respond to realize the potential benefits of the IoT. In addition, need to be addressed, including infrastructure readiness, market and investment incentives, the need for technical skills, resources and political needs and challenges of implementation in less developed regions unique.

4. Literature survey:

In 2010, Rolf H. Weber projected “Internet of Things – New security and privacy challenges.” The Internet of Things, a global technical architecture emerge on the Internet facilitating the exchange of goods and services in the global networks of the supply chain

has an impact on the security and privacy of the parties involved. Measures to ensure the architecture of resilience to attacks, data authentication and access control and customer privacy must be established. An adequate legal framework should take the underlying technology into account and would be better prepared by an international legislature, which is complemented by the private sector to the specific needs and is easily adjustable. The contents of the respective legislation should include the right to information, measures prohibiting or restricting the use of the mechanisms of the Internet of things, rules on the IT-security law, provisions promoting the use of mechanisms the Internet of Things and the creation of a working group to do research on the legal challenges of IoT.

With the emergence of an Internet of things, new regulatory approaches to ensure its confidentiality and security are needed. In particular, attacks are to be intercepted, the authenticated data, controlled access and customer privacy (individuals and corporations) guaranteed. The nature of the IoT requires a diverse and differentiated legal framework that sufficiently takes into account the whole, verticality, ubiquity and the technicality of the IoT. Geographically limited national legislation does not seem appropriate in this context. However, self-regulation as it was applied until now, may not be sufficient to ensure the confidentiality and security effective, either. Therefore, a part of the key principles of substance determined by law at the international level, complemented by the private sector with more detailed regulation seems to be the best solution. With such a framework, general pillars of regulation could be set for everyone, which are then able to be completed by the persons concerned in a way that suits their current needs. [1]

In 2011, Tobias Heer, Oscar Garcia-Morchony, Rene Hummen, Sye Loong Keohy, Sandeep S. Kumary, and Klaus Wehrle present “Security Challenges in the IP-based Internet of Things.” A direct interpretation of the term Internet of Things refers to the use of standard Internet protocols for human thing to another thing or the thing in communication in embedded systems. Although security needs are well recognized in this field, it is not yet fully understood how IP security protocols and existing architectures can be deployed. In this research, the authors discuss the applicability and limitations of Internet protocols and security architectures that exist in the context of the Internet of Things. First, they give an overview of the deployment model and the overall security needs. They then present challenges and requirements for IP security solutions and highlight the specific technical limitations of IP security standard protocols.

From the life cycle of a thing in an application LAC, this paper examined the architectural

design for a secure IP-based Internet of things and challenges with a focus on IP security standard protocols.

A first conclusion refers to the fact that the security architecture should be the life of a thing and its capabilities. This includes aspects such as how a security domain is created, the need for third-confidence in this process, or the type of applied protocols. Another important condition for an architecture is that it should evolve in ad hoc security domains small scale of things in large-scale deployments, potentially on several security domains. Security protocols should also consider the nature of the limited resources of things and heterogeneous communication models. As regards the first aspect, security protocols should include lightweight security mechanisms that are feasible to run on small things. To enable security protocol variants and specific to the field from start to finish, the protocols must be adapted to support translations by bridges. The safety of the group must be considered as well, since the IoT brings communication patterns that are unusual in traditional networks, and are therefore not sufficiently supported by Internet security protocols throughout. The design of the Protocol should also take into account the effect of the fragmentation of security packages, with particular emphasis on possible DoS attacks. [2]

In 2012 Jing Liu and Yang Xiao, C. L. Philip Chen presented “Authentication and Access Control in the Internet of Things.” Due to the inherent vulnerabilities of the Internet, issues of security and confidentiality should be investigated and dealt with before the Internet of Things is widely deployed. This article mainly analyzes the existing authentication and access control methods, then he designs a possible for the Internet of Things. This article mainly analyzes the existing authentication and access control methods, then he designs a possible for the IoT. The analysis results show that our approach can prevent attacks such as eavesdropping, man in middle attack key control, and replay attacks.

Authentication is a protocol processing communications procedure. In the IoT, secure communication must be built from a 'thing' and other such proceedings. The identity of the second "thing" or claims of the object should be compatible with that one first claims. Identity information becomes claimed one message.

Based on this message, the authors verify the identity of "things." The goal for both communication partners to implement the authentication protocol is to have a solid communication in the upper layer (e.g., the application layer). To do this, usually the authentication protocol has several sub- tasks such as setting up identification of the key, or the keyboard switching and consultation. In an authentication process of the claimer identity

can be achieved through the identification of the message. In the key establishment protocol authenticated, the establishment of key materials are also important protocol messages, part of the authentication of the entity.

In this article, the authors focus on establishing simple and effective secure key based on ECC (Elliptic Curve Cryptosystem). For access control policy, we adopt based RBAC (Role-Based Access Control) authorization method using the role of the particular thing (s) and application (s) in the associated IoT network. [3]

In 2013, Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig, Georg Carle presented "DTLS based Security and Two-Way Authentication for the Internet of Things." In this article, the authors introduce the first authentication security system fully implemented two ways for the Internet of Things (IoT) based on existing Internet standards, in particular the Protocol Datagram Transport Layer Security (DTLS). Based on an established standard, existing implementations, engineering techniques and security infrastructure can be reused, thereby allowing easy absorption of security. Proposed security system is based on RSA, the most widely used public key cryptography algorithm. It is designed to operate on standard batteries that provide communication UDP / IPv6 network for low power Wireless Personal Area Networks (6LoWPAN). Implementation of DTLS is presented as part of a system architecture and feasibility of the system (low overheads and high interoperability) is further demonstrated through a thorough assessment on a suitable hardware platform for the Internet of Things.

The authors have developed a standard security architecture based on the two-way authentication for the IoT. Authentication is performed during a handshake DTLS fully authenticated and based on an exchange of X.509 certificates with RSA keys. The in-depth assessment, based on real systems IoT, shows that their proposed architecture provides message integrity, confidentiality and authenticity with affordable energy, latency and memory after the end of the head. This shows that DTLS is a possible security solution for the emerging IoT. They consider a handful of fully authenticated hand with enhanced security with 2048 bit RSA keys possible for sensor nodes equipped with a TPM chip, since a basic handshake fully authenticated RSA consumes as little as 488 mJ. The memory requirement of less than 20 kb of RAM is well below the 48 KB of memory offered by sensor node. Sensor nodes without a TPM chip renounce protection against intrusion, but can still make a DTLS handshake based on ECC that could be realized on the platform with a little over

100 mJ of energy consumption. Previous work has demonstrated techniques to minimize packet headers to similar protocols.

In 2014, John A. Stankovic presents “Research Directions for the Internet of Things.” Many technical communities are vigorously pursuing research topics that contribute to the Internet of Things (IoT). Today, sensing, actuation, communication, and control become increasingly sophisticated and pervasive, there is significant overlap in these communities, sometimes slightly different perspectives. A fundamental problem which is ubiquitous in the internet today that must be resolved is the face of security attacks. Security attacks are problematic for IoT because of the minimum capacity "things" (devices) used, the physical accessibility of sensors, actuators and objects, and open systems, including the fact that most wireless devices communicate. The security problem is compounded because of transient and permanent failures are common random and failures are vulnerabilities that can be exploited by attackers. However, considerable redundancy is available creates a potential for designing applications to continue providing their services specified even in the face of failures. To meet the realistic system requirements arising from long-term, unattended operation, the IoT applications must be able to continue to function satisfactorily in the presence of, and effectively recover against security attacks. Solutions may require download of new code and this itself is open to security attacks. The system must also be able to adapt to new unforeseen attacks when the system was deployed. These problems are beginning to be addressed by work such as that found. In the system operates with a level of support, including basic strong attack detection capabilities. Once an attack is detected, then the reaction occurs, by self- healing.

To heal security attacks, a system must detect the attack, the attack diagnose, and deploying against measures and repairs, but do all this in a light way because of the types of small capacity devices involved. Most security solutions for the mainframe today require heavy calculations and large memory requirements, so that solutions for IoT are the main challenges of research. Ideally, for an answer, given the real-time nature of many IoT, detection, against measures and service must operate in real time as part of an enforcement architecture of self-healing. Sometimes healing requires a new program, for example, when an unexpected attack occurs. In these cases, healing instructions must be firmly (with authentication and attestation) issued to the appropriate nodes and programs running node must be modified by the execution of architecture. It is likely that the important material support will be needed to provide the encryption, authentication, attestation, and alter key

evidence. Even if new devices are secured to date, on existing devices will prove difficult. [6]

In 2015, Flauzac Olivier, Gonzalez Carlos, Nolot Florent, presented "New Security Architecture for IoT Network." The authors explain the concept of security architecture for the Internet of Things (IoT) -based networking software defined (SDN). In this context, based architecture RPS works with or without infrastructure, the authors call NRS-Domain. This work describes the operation of the proposed architecture and summarizes the ability to achieve the security of a more efficient and flexible network with RPS. An overview of PHI security existing applications were discussed and addressed its issues, presenting the architecture of a new IoT system. In this article, considered the network access control and monitoring of world traffic for ad-hoc networks. Finally, highlight the architectural design of choice for RPS using OpenFlow and discuss their implications on performance.

This article gave an overview of a new basic network architecture of SDN with distributed controllers. In addition, the solution can be used in the context of ad hoc networks and IoT.

First, the authors presented a new architecture with multiple controllers RPS equal interaction. Second, they have proposed an architecture that is scalable with multiple areas of PHI. In each area, they can network with or without infrastructure and each controller is responsible only for its domain. Communications between the areas is made with special controllers called border controllers. These advanced controllers must work in a new interaction distributed to ensure the independence of each domain on failure. The authors adopt an architecture to guarantee the security of the entire network with the concept of integrated safety gate in each controller to prevent attacks. [7]

5. Conclusion and future work:

After In this survey paper proposed the bird eye view on different type of IOT, also represent the different IOT techniques used in previous research. Now a days IOT and its different type is burning topic in between researcher. In this paper shows the main technical issue of IOT and also describe the technical challenges in the IOT establishment. After the discussion of technical problem focus on the main technology of IOT used. At the last shows the review of different previous papers of different researchers. In future try to develop a new security protocol for IOT and improve the security issues of IOT and improve the quality of IOT. This protocol is based on network layer. These works try of

improve the IOT.

6. References:

(1) Rolf H. Weber, "Internet of Things – New security and privacy challenges", computer law & security review 26 (2010) 23 – 30, Published by Elsevier Ltd. doi:10.1016/j.clsr.2009.11.008.

(2) Tobias Heer, Oscar Garcia-Morchony, Rene Hummen, Sye Loong Keohy, Sandeep S. Kumary, and Klaus Wehrle, "Security Challenges in the IP-based Internet of Things", Springer Journal on Wireless Personal Communications, December 2011, Volume 61, Issue 3, pp 527-542.

(3) Jing Liu and Yang Xiao, C. L. Philip Chen, "Authentication and Access Control in the Internet of Things", 32nd International Conference on Distributed Computing Systems Workshops, IEEE DOI 10.1109/ICDCSW.2012.23.

(4) Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig, Georg Carle, "DTLS based Security and Two-Way Authentication for the Internet of Things", Elsevier Journal of AdHoc Networks in May 2013.

(5) Omar Said, "Development of an Innovative Internet of Things Security System", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.

(6) John A. Stankovic, "Research Directions for the Internet of Things", National Science Foundation under grants CNS- 1239483, CNS-1017363, and CNS-1319302. Copyright (c) 2014 IEEE.

(7) Flauzac Olivier, Gonzalez Carlos, Nolot Florent, "New Security Architecture for IoT Network", International Workshop on Big Data and Data Mining Challenges on IoT and Pervasive Systems (BigD2M 2015), s. Published by Elsevier, Science Direct, Procedia Computer Science 52 (2015) 1028 – 1033.

(8) Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, "Twenty security considerations for cloud- supported Internet of Things", Internet Of Things Journal, IEEE 2015.

(9) Z. Shelby, K. Hartke, C. Bormann, B. Frank, Constrained Application Protocol (CoAP), IETF draft, RFC Editor (March 2013). URL http://tools.ietf.org/html/draft-ietf-core-

coap-14

(10) S. Dawson-Haggerty, A. Tavakoli, D. Culler, Hydro: A Hybrid Routing Protocol for Low-Power and Lossy Networks, in: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Smart Grid Comm, 2010, pp. 268-273.

(11) D. Raymond, S. Midki_, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, Pervasive Computing 7 (1) (2008).

(12) Luk, G. Mezzour, A. Perrig, V. Gligor, MiniSec: A Secure Sensor Network Communication Architecture, in: Proceedings of the 6th International Conference on Information Processing in Sensor Networks, IPSN, 2007, pp. 479-488.

(13) V. Gupta, M. Wurm, Y. Zhu, M. Millard, S. Fung, N. Gura, H. Eberle, S. C. Shantz, Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet, Pervasive Mob. Comput. 1 (2005) 425-445.

(14) W. Hu, H. Tan, P. Corke, W. C. Shih, S. Jha, Toward Trusted Wireless Sensor Networks, ACM Transactions on Sensor Networks 7 (2010) 5:1-5:25.

(15) H. Chan, A. Perrig, D. Song, Random Key Predistribution Schemes for Sensor Networks, in: Proceedings of Symposium on Security and Privacy, 2003, pp. 197-213.

(16) W. Jung, S. Hong, M. Ha, Y.-J. Kim, D. Kim, SSL-Based Lightweight Security of IP-Based Wireless Sensor Networks, International Conference on Advanced Information Networking and Applications Workshops (2009) 1112-1117.

(17) S. Raza, T. Voigt, U. Roedig, 6LoWPAN Extension for IPsec, in: Proceedings of the Interconnecting Smart Objects with the Internet Workshop, 2011.

(18) S. Raza, T. Voigt, V. Jutvik, And Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15.4 Security, in: Proceedings of the IETF Workshop on Smart Object Security, 2012.