Survey of Intrusion Detection Systems towards an End to End Secure Internet of Things

Audrey A. Gendreau, Ph.D.[1], Michael Moorman, Ph.D.[2]

[1]College of Innovation and Technology, Florida Polytechnic University
Lakeland, FL., USA
agendreau@flpoly.org

[2]CS & CIS, Saint Leo University
Saint Leo, FL., USA
michael.moorman@saintleo.edu

***Abstract*—The Internet of Things (IoT) is one of the largest technological evolutions of computing; by 2022 it is estimated that a trillion IP addresses (objects) will be connected to the Internet. The obscurity and low accessibility of many of these devices in this vast heterogeneous network will make it difficult to holistically monitor information flow. Nonetheless, to safeguard networks, unauthorized intruders must be detected within the constraints of each type of device or subnetwork before any system information can be disseminated.**

In this paper, a survey of the Intrusion Detection Systems (IDS) using the most recent ideas and methods proposed for the IoT is presented. To understand and illustrate IDS platform differences and the current research trend towards a universal, cross-platform distributed approach, the survey starts with an historical examination of intrusion detection systems. This examination of the foundations of IDS research based on the components that make up the IoT is followed by a look at the current holistic trend and an analysis of these schemes. Finally, guidelines to potential IDS in the IoT are proposed before identifying the open research problems.

***Keywords*— Internet of Things, IoT, Cloud, Wireless Sensor Networks, WSN, Intrusion Detection System, IDS, Radio Frequency Identification, RFID, Cell Phone**

I. INTRODUCTION

While the computing epochs defined by the mainframe, Personal Computer, and now the ubiquitous age have been delineated, there is disagreement over the novelty, and thus, legitimacy of the definition of the Internet of Things (IoT) as a new era in computing history. To address this issue of what it deemed a "fuzzy" definition the IEEE IoT Standards Association has developed an eighty-six-page document titled "Towards a Definition of the IoTs" [1]. A part of this skepticism may be because as shown by the document's focus on organized markets and stakeholders, in the delineation of the IoT less emphasis has been placed on the world-wide automation of machine-to-machine (M2M) or machine-two-user (M2U) connections which are occurring by ordinary people to make their everyday tasks easier. Furthermore, non-utilitarian objects like art are not considered. Instead, attention is on the increased commercial automation occurring in more sophisticated applications; such as, heart monitoring implants, bio-chipped humans and animals, futuristic firefighter sensing suits, and automobiles with built-in sensors. Previously thought to be stagnant because of the dependency upon the creation of applications like these that adhere to a set of complex standards, e.g. efficient, self-reliant, management and monitoring capability, robust, scalable, adaptable, reliable, and trustworthy [2], the growth of the IoT has surged with the emergence of low-cost microcontrollers[3][9]. In this new era in computing history, Internet edge nodes are no longer limited to consumer and industrial uses for profit driven offerings, but are also being used for unique, individualistic, undocumented first-time creations [3][9].

Empowering this phase are not only the advancements made by lower cost microcontrollers, but the programmability and capability of embedded device development has vastly improved. This is because the most popular embedded prototyping platforms use commonly known programming architectures. The Arduino, a very popular platform, comes with a Windows distribution, and thus, a slim version of .NET and facilitates C# and C client/server development [3]. Moreover, the Arduino manufacturers in partner with Adafruit [4] make Wearables, an embedded device designed to be sewn into clothing. While embedded devices are usually known for their physical limitations these ten dollar microcontrollers have 32-bit CPUs and 48KB of onboard RAM. A printed circuit

978-1-5090-4052-0/16 $31.00 © 2016 IEEE
DOI 10.1109/FiCloud.2016.20

IEEE computer society

board (PCB) for the microcontroller with an Ethernet card using a familiar programming architecture is less than fifty dollars. Overall, this ease of development and affordability trend of the IoT era is continuing. While Arduino is a product of Italy, the open source platform has enabled the production of imitations at reduced prices. Mini computers compete with the Arduino microcontroller platform. The Raspberry Pi and BeagleBone Black are both Linux distributions with Python scripting (in addition, Raspberry Pi supports Java).

To underscore the level of enablement in this era to build a system that can respond to a physical phenomenon, consider that less than a decade ago, the state-of-the-art WSN technology, a major component in the IoT, was manufactured by Crossbow. To implement an application on a fixed hardware Crossbow platform required reading a 100 page programming manual in order to understand the nesC programming language, and referencing another manual to learn about the TinyOS onboard operating system. At the time of writing this paper, three legacy Crossbow wireless sensors with an additional three-hundred dollar Internet component could be purchased for slightly less than seven-hundred dollars from Memsic [5]. Contemporary Arduino embedded devices fitted with a twenty-dollar XBee [6] communication module create a mobile embedded sensing device that is less than fifty dollars and easier to program using the discussed above common program platforms.

Furthermore, with the additional features facilitating hardware design, these first time creations can become sophisticated mobile embedded devices capable of reporting on a variety of physical conditions over the Internet for much less effort and cost than previous systems. For example, the WSN protocol, ZigBee, is implemented as part of the embedded code for the XBee transceiver. The coordinator (or, sink) in the ZigBee standards is the node toward which all the data is funneled. Although two separate networks pose a cross contamination security risk, a dual purpose gateway to the Internet and WSN coordinator can be constructed using a stack of three PCBs with the upstream link connected to an Ethernet port and the downstream link facilitated by an XBee communication module [3].

Moreover, as anticipated for this era [2], analysis of sensor data streams in real time is being conducted by IoT data-based cloud services. Supporting automated sensor measurements, Xively recruited volunteers with Geiger counters to facilitate radioactive monitoring of the Yokashima nuclear power plant [6]. Another example of a cloud service is Sparkfun [40]. Using Sparkfun a maximum of 50mb for each stream is free before it is deleted. These technologies are becoming more commonplace and, (as noted previously), by 2022 it is projected that a trillion devices, many of which will be vulnerable undocumented first-time creations, will be connected over the Internet.

Lastly, not previously considered but made possible with the lower costs and ease of development, there is a growing Do-It-Yourself (DIY) electronic prototyping community. This group is driving the development of things without regard to the adoption of formally thought out standards for IoT expansion, which are essential for security of the network. Furthermore, there is a strong and growing maker movement, in which high school and college students are invited to hack an invention; hack in this context means to invent a *thing*. One example of this movement can be observed in competitions; Major League Hacking (MLH), the organization that hosts Hack the Planet and another 150 similar competitions each year, recently, invited young people to the Silicon Valley to compete for the best invention [38]. While these first time creations include everything from electronic art to utilitarian applications, when connected to the Internet, the potential for exploitation for attacks is much higher.

Since these unique applications and embedded devices, not complying with the IoT standards have limited visibility and are remotely accessible, security in the IoT is a critical issue. Moreover, the layers of protection are constrained by the devices' own hardware and software limitations making them easy targets for an attack. Recently, a botnet (illegal remote control of hosts) took over almost 1000 closed-circuit television cameras (CCTV) [7]. The Distributed Denial-of-Service (DDoS) attack succeeded by flooding the network with http get requests. Similarly, the authors attributed the CCTV exploitation to a lack of visibility and capability for remote access. Other less visible and remotely accessible devices that have been hacked include refrigerators, baby monitors, and stoves [7][8]. In a paper by Dlamini et al. the authors illustrate how a botnet could compromise the power grid in a region in South Africa by switching stoves of an entire suburb to maximum power for four hours [8].

Today and for the foreseeable future, not only will it be difficult to protect all of the known device types and their owners, but it will be especially difficult to defend the more vulnerable undocumented ones. To safeguard the IoT, an all-inclusive approach to IDS application in the IoT is the primary focus of this paper. However, in order to understand the importance of the new trend in the IoT research community towards a more holistic IDS approach, the past platform constrained systems and current, open problems are provided.

A. Guide to the Paper

Section II presents a brief review of the IDS literature for a foundation of the presented work. It specifies the evolutions and history of IDS in the components of the IoT. Section III presents an account of the current trends of IDS in the IoT and Section IV is an overview of suggested directions for the IoT. Section V presents a summary of the conclusions as well as avenues for future work.

II. Intrusion Detection Systems

The purpose of an intrusion detection system (IDS) is to detect unauthorized access. Some of these systems and networks that need access protection include: wide area networks (WANs) and clouds, local area networks, (LANs), ad hoc networks, wireless local area networks (WLANs), and wireless personal area networks (WPANs). In the

WPAN family the three more common networks include: wireless sensor networks (WSNs), mobile phones, and radio frequency identification (RFID). The IDS on these systems and networks can broadly be categorized according to the detection techniques utilized, e.g. anomalies, stateful packet examination, or rule-based.

A. WANs, LANs, WLANs, Ad Hoc Networks

The concept of *intrusion detection* began in the 1980s; during the next twenty years, host-based IDS processing audit logs grew into automated network IDS on wireless systems. One of the earliest works on intrusion detection was completed for a government agency by Jim Anderson [10], a founder of IDS, focusing on ways to improve security auditing and surveillance systems. In his final report, "Computer Threat Monitoring and Surveillance", Anderson suggested ways to scrutinize audit logs for intrusion detection. The audit logs on which he based his report were originally targeted for employees performing the data processing that oversaw different types of batch processes. Anderson examined the logs to analyze threats to files on host machines and, using the logs, he differentiated normal use from anomalies to determine any unauthorized access to the data.

Like Anderson, Denning [11] focused on processing audit logs for security violations by scanning for anomalous use. Later, Lunt and Jagannathan [12] used this approach to create a host-based IDS that determined normal behavior from historical audit logs before applying it to current audit logs to detect and identify potential intrusions.

In the 1990s the authors Heberlein, et al., [13] extended Denning's host-based intrusion detection model to include network monitoring. The proposed IDS analyzed network traffic and compared current and past behavior to discover anomalies and thus intruders.

By 1993 wireless computing had become more popular, as users understood the freedom (but not the potential security issues) provided by going wireless. A well-known paper on ubiquitous computing by Mark Weiser [14], the father of ubiquitous computing, forecast an age when machines would be transparently computing in the human world to make everyday tasks easier, which could be argued to be a foreshadowing of the IoT. However, researchers understood the potential vulnerability of going wireless. Bharghavan and Ramamoorthy [15] approached wireless intrusion prevention by suggesting a scheme to provide authentication and message security. This is particularly important because it is an early paper that addressed the manner in which the issues of limited hardware, mobility, and self-sufficient nodes impact security.

In 1998 the Defense Advanced Research Projects Agency (DARPA) benchmarked current IDS systems; even in the best systems the detection rate was considered too low, especially for detection of new attacks [16]. Subsequent to the DARPA study, the turn of the 21st century was marked by another well-known paper on intrusion detection by Tim Bass [17]. In this paper, Bass proposed to improve detection in the whole cyberspace or WAN by making inferences using data supplied from many different systems.

And, in response to the DARPA study on low detection rates, and because of the differences between wired and wireless ad-hoc networks, Lee and Zhang [18] proposed an agent-based distributed IDS for wireless ad-hoc networks. These authors pointed out that in a wired network, an IDS must be strategically placed on switches, routers, and gateways to glean information from the visible traffic points. To address these same issues on a wireless ad-hoc network, Lee and Zhang proposed a distributed agent-based approach to intrusion detection.

B. WSNs

Prior to 2006, there was a time when the difference between WSNs and ad-hoc networks was not delineated; for example, in a paper by Iheagwara, Blyth, and Bennett [19], identical specifications for intrusion detection development on both mobile and ad-hoc networks were provided. The type of wireless network was not differentiated in their report. In fact, they reiterated that their IDS specifications for a WSN were also effective for other wireless environments. However, shortly after this paper, the field of IDS research on ad-hoc networks began to mature, and the differences between wireless platforms were recognized. In a noteworthy paper by Roman, Zhou, and Lopez [20], the authors pointed out that an IDS for an ad-hoc network could not be applied directly to a WSN, and the need to develop different approaches was noted. Today, there are many approaches to WSN IDSs as outlined in a recent paper by Butun et al.[21]. The authors analyze current WSN IDSs and discuss viable schemes. The WSN IDSs categorized include: hierarchical, distributed, statistical, game theory, anomaly, and trust. While energy was emphasized as a primary concern in WSNs, and thus, an important design issue. They suggest that mobile platforms use a hybrid approach of distributed and cooperative technology; stationary schemes use a centralized approach, and of the WSNs presented the authors selected the cluster based schemes that were scalable.

C. Mobile Phones and Cloud-based Solutions

Today′s tech users are more attached to their devices than ever; smart phones are replacing the personal computer (PC) for performing financial transactions and browsing the Internet, as well as using social media, and monitoring one′s health. Moreover, antivirus software traditionally thought of for personal computers (e.g., Avast, Kaspersky, and McAfee) are now also available for cellphones. Phones are now threatened by the same common place personal computer security issues (i.e., worms, Trojan horses, viruses) that have been considered part of the landscape of the personal computer [22]. However, bound by resource limitations they are even more vulnerable than personal computers, creating an additional need for more research in security of the IoT and cloud-based solution services. In a paper by Khune and Thangakumar [22] the authors proposed an alternative cloud-based intrusion detection system for

Android smartphones. Their solution was to use the cloud as a way to alert a phone of an intruder and then afterwards use the cloud to recover from the attack. As an alternative to conventional antivirus software, this approach conserves battery, bandwidth and computational power. However, this would only be a partial solution as, according to a paper by a number of researchers from AT&T labs [23] many other signatures for smart phone malware are difficult to detect because they change frequently. Additionally, some malware attacks are meant to extract money fraudulently, and thus the attack vector may not involve software, i.e. texting scams. AT&T labs researchers have also found success in anomaly detection using network-based clustered communication patterns. They showed how this technique can be used to detect a malicious campaign motivated by financial gains. Their solution is scalable, signature free, and holistic. Turning off one phone does nothing to a campaign of this magnitude, involving multiple users and devices, but having the capability of eliminating multiple pieces of the cybercriminals′ infrastructure could have the potential to end it at a system level, rather than a user level.

D. RFID

Similar to smart phones and WSNs, and restricted by their physical size, RFID applications have computational limitations. The technology is a combination of the RFID tag and the reader which uses electromagnetic radiation to transport and recognize data. Less than a decade ago, with the advent of more RFID use cases in manufacturing, and with the demand by government and corporations for more sophisticated tracking capabilities of inventory, over more traditional inventory shipping lists, intrusion detection research became more prevalent, although to date there is still only a limited number of published RFID intrusion detection experiments in the professional literature. Some of the research published includes a proposal by Thamilarasu and Sridhar in 2008 [24] that suggest a network approach to intrusion detection by detecting anomalous behavior in the reader and middleware layer. While in 2009, Yang applied intrusion detection to Radio Frequency Identification technology using a modified immune clustering model to guide the search of a chaotic strategy [25]. A third proposal in 2010, by Hao-yan suggests the implementation of snort, a long standing state-of-the-art IDS, to use its statistical analysis model on the IDS database that stores the RFID data [26]. Recently, with the growth of more commonplace use of RFID technology new research has surfaced to provide an experiment on detecting jamming attacks [27]. This is a type of DoS attack conducted by applying radio interference to an RFID system. The network-based detection engine used an artificial immune system to detect the jamming attack prior to it stopping the communication, after losses occurred.

III. IoT CURRENT TRENDS IN IDS

As the above research has demonstrated there are important differences between WANs (clouds), LANs, WLANs, Ad Hoc, WSNs, mobil phones, RFID, and other WPAN technologies as well as differences in methodologies used to detect intrusions. These differences directly affect IDS implementation. For example, unlike a LAN, because a node in a WSN can be removed, reprogrammed, and put back into the network, a WSN does not want its more vulnerable nodes (e.g. sink and nodes close to it) to be designated as the IDS agent. Conversely, a less hardened legacy box on a more traditional LAN would likely host an IDS.

While these earlier IDS proposals focused on the specific components, within the last five years IoT research has matured enough to realize the need for unilateral intrusion detection support across the different technologies. This approach will continue to evolve over time, and will also need to take into consideration the maker movement and the DIYs, in a way that can harness both the potential for innovation and the threat this segment may pose by driving the development of things without regard to any industry standards for IoT expansion, which will be essential for security of the network.

As previously discussed, Tim Bass suggested a holistic cross-platform approach for detecting unauthorized access in the whole cyberspace should involve evaluating inferences from multi- perspectives. For this reason, the *Interaction Ability* as first proposed by Shaiek et al. [28] as a critical parameter in a deployment metric of an IDS, was used to rank the level of the holistic detection intelligence of the reviewed IDSs. It provides a multi-perspective view of the IDSs interaction with the following TCP/IP suite's four network service layers: Network Interface, Internet, Transport, and Application layers. Moreover, the TCP/IP layers can be mapped to functionally similar ZigBee WSN standards (e.g. Physical, 802.15.4 MAC, Network, and Application) and as an encapsulation or otherwise in 6LoWPAN [29]

The ability to interact with protocol characteristics at various layers in the network is not the same thing as the traditional host or network IDS placement categories. The Interaction Ability is an indicator of the ability to perform real time analysis, and generate a timely response at each layer as needed. At the higher layers an IDS is more energy efficient and responsive, because there are less packets to examine. In a node, not all of the received packets are destined to the application layer. For the same reason, the IDS detection ability is more accurate at the lower layers. All of the messages destined to the different layers are first received at the lowest layer.

As originally proposed, the Interaction Ability is computed by adding one for each layer the IDS supports. As a multi-perspective holistic indicator, ideally the IDS would interact with all the service layers for a total value of four. In Table 1, based on our understanding of the literature, the reviewed IDSs proposed for the IoT are ranked by their Interaction Ability. Consequently, using this technique for analysis the IDSs that appear to use the most holistic, cross-platform approach are anomaly detection techniques listed at the bottom of the table. In the following two sub-sections, the IDSs surveyed are organized based on their resulting Higher (2, 3, & 4) or Lower (1) Scored Interaction Abilities.

Author	Interaction Ability Score	Detection Technique	Features
Batalla & Krawiec [35]	TCP/IP Internet Score= 1	Not specified, focus is throughput.	Processing large data streams for real time performance of IDS.
Kasinathan et al. [37]	TCP/IP with 6LoWPan Internet Score= 1	Rule	6LoWPAN Integration
Kasinathan et al. [38]	TCP/IP with 6LoWPan Internet Score= 1	Rule	Extend [37] 6LoWPAN Integration
Kafle et al. [33]	TC{/IP Application, Transmission Score= 2	Not specified, focus is response time.	ID-based and real-time processing
Jun & Chi [34]	TCP/IP Application, Transport, Internet Score= 3	Anomaly	Improved response time to security events.
Gupta et al.[32]	TCP/IP Application, Transport, Internet Score = 3	Anomaly	Deployable to all nodes, reacts to new attacks, mobile.
Caiming et al. [31]	TCP/IP Application, Transmission, Internet, Network Inter. Score = 4	Anomaly	Detect new attacks and adaptive

Table 1: Analysis of recent IDS schemes for IoT

A.IDS with Higher Interaction Ability Values

At the beginning of 2011, the ideology of IDSs began to change as the research began to not target individual or related components, but the whole IoT. In one of these experiments, Liu et al., applied the mechanisms of artificial immune systems to IDSs3 in the IoT [31]. The researches postulated they could use an approach similar to the immune system response of the body for intrusion detection. Memory Detectors are software simulating antigens which act as immune cells in the human body recognize attacks. The researcher tested a trained Memory Detector to use its gene (attack signature) to match an antigen (attack). Each Memory Detector was related to an attack that had been cataloged in the attack library. The authors mathematically analyzed the theory, and found that this technique may be able to address the problem of detecting millions of intrusions in the whole of cyberspace. Potentially interacting with each layer in the network stack, it is important how the application would be distributed as agents in order to implement the whole system.

More recently, there has been a proposal for Computational Intelligence (CI) based systems which are adaptable and react to new situations by applying reasoning without relying on users [32]. Examples are artificial neural networks, evolutionary computation, artificial immune systems, swarm intelligence, and fuzzy logic. Using a three tier architecture for monitoring, applying computational intelligence, and reporting intrusions, the IDS tracks the IP addresses of the source messages and stores it against their network or system patterns. While promising, the design has not yet been implemented, and needs more investigation. It presumes that every device will have an IP address. WSNs, not configured for 6LoWPAN, use alternative protocols than the TCP/IP suite and don't have IP addresses. Also, focused on the logical address it is not clear how much it would interact with the physical layer which is based on the MAC address. Finally, as a holistic approach it categorizes its offerings as either network or host based. Seemingly, a truly holistic approach would not differentiate between these categories.

Another approach used by Kafle et. al., addressed the issue of integrating non IP networks by assigning unique identifiers to every object [33]. The ID-based communication in heterogeneous networks named the Identity Sublayer was embedded in the transmission layer for better real-time performance than traditional IDS.

Quite recently, in 2014 Jun et al. developed a Complex Event Processing (CEP) engine for real-time pattern detection amongst the different components in the IoT. It was benchmarked against an IDS that first stores, and then matches the data with a rule. They found that their approach was more CPU intensive, but consumed less memory. Effectively it proved better real-time performance [34].

B.IDS with Lower Interaction Ability Values

The Internet (Network) layer is an ideal place for a holistic approach to a rule based detection engine because

the lower layers depend on the hardware, and are less abstracted. The following is a review of two different IDSs operating at the network layer. The first work utilizes the traditional TCP/IP suite (Batalla & Krawiec) [35] and the second experiment uses the TCP/IP suite with 6LoWPAN (Kasinathan et al.) [36] [37].

Batalla & Krawiec [35] propose a type of service-orientated architecture embedded in the TCP/IP Internet layer to enable object communication irrespective of their hardware or software platforms. An important technique utilized involved registration of services and objects in order to search and deliver the information related to them. It avoided overload by using hierarchical designated routers to filter only necessary information to the parent node. Decoupling the identification of services/objects from their location may be ideal in the future when the embedded device technology is more sophisticated, and the potential for what might be termed WildCard IoT devices, or non-standardized non-compliant objects will be even more wide spread. However, the current 6LoWPAN technology was not examined. Furthermore, it was expected that the controller in the sensor network would be the interface to the other sensor devices without (from what we can tell) consideration for the rest of the WSN.

Another promising DoS detection framework for IoT intrusion detection and security integrated was an open source IDS named *Suricata* modified for a IPv6 over low-power personal area network (6LoWPAN). The 6LoWPAN protocol provides IPv6 identity to objects that otherwise don′t have an IP based protocol [36]. A large part of this work was the packet analysis that was integrated into the IEEE 802.15.4 network layer. The DoS test showed promise. A follow-up of Kasinathan demonstration was to modify the originally open source code to integrate an advanced event monitoring system [37]. Also, they added the capability of the IDS to monitor larger networks than previously possible by the original DoS detection architecture. The enhanced detection engine, Suricata, added IEEE 802.15.4 and 6LoWPAN decoders to inspect incoming packets and trigger alerts based on rules programmed [37].

IV. SELECTION OF IDS FOR IOT

Based on the review of this research the following observations have been made. 1) While the IoT can be thought of as a vast heterogeneous network, the problem is that it lacks complete interoperability between its parts. Still relatively new, with limited functionality for WSNs over the Internet, 6LoWPAN has been proposed as one solution to this issue. It replaces the layers above the WPAN protocol 802.15.4 with a suite of Internet capable standards to facilitate IPv6-based connectionless communication across the Internet. As a comprehensive solution it encapsulates existing WPAN protocols above the network layer. Thus, the DoS [36] detection architecture implemented in the network layer of 6LoWPAN seemed to be the most interoperable approach at this time. 2) As expected to be successful in detecting attacks, the detection system itself must be immune to attacks [31]; as such, it must adhere to the IoT standards. These unique standards embody self-reliant characteristics which are inherent to anomaly detection as suggested in [31][32]. Contrary, rule and stateful packet inspections are not completely autonomous, and require some human intervention. Furthermore, anomaly detection is a more holistic, cross-platform approach as shown by the holistic analysis using the interaction ability. 3) Unlike the immunity approach, it is of our opinion that the actual protocol analysis should be abstracted to a more generic form. For example, the storage of IP addresses in [31] should be matched to an alternative form of identification as experimented with in [33].

Accordingly, we draw the conclusions that a Hybrid IDS integrated into the 6LoWPAN protocol that can contribute to some degree to each of the four service layers, exhibit a multi-perspective anomaly-based intelligence, and abstract the details of the protocol analysis, would be the most promising intrusion detection system for the future IoT.

V.CONCLUSIONS AND FUTURE TRENDS

A. Conclusions

With affordable and easily constructed programmable embedded devices, DIYs and a spirit of young entrepreneurs paradigm is being promoted outside of the corporate and industrial realms. These distinctive changes are definitive of the IoT computing era. With a wide variety of architectures ranging from undocumented ad hoc embedded devices to very structured ones adhering to the standards, the IoT is burdened with additional security issues. For this reason, a ubiquitous IDS joined at time of network access, interacting with each service layer, will gain importance as an ever-increasing number of less visible but Internet accessible applications are created.

B. Future Work

Within the last five years, the concept of a holistic architecture for IDS in the IoT has begun to be explored. Still in its infancy, this trend will grow and continued evaluation of IDS implementation at each service layer as well as benchmarks between systems will be important to the safety of the machines and their owners. Moreover, the prevention of unauthorized access to the IoT will depend on the intrusion detection capability of the most vulnerable components which are the embedded devices constrained by limited computational capacity and power – a long standing open problem for WSNs. Another issue is that the DIY user group is not trained in security. For example, the default userid and password of a Raspberry Pi microcontroller; Raspberry, Pi respectively is used. Also, rebooting microcontrollers for software updates is less frequent because it interrupts data collection of the monitored physical phenomena. For this reason, education and policy will also need to be established as part of the effort towards end to end IoT intrusion detection.

VI. ACKNOWLEDGEMENT

We would like to give special thanks to Michael Gendreau for his insight into the Arduino DIY community.

REFERENCES

[1] IEEE, Towards a Definition of the IoT. May 2015 Retreived December 1, 2015.

[2] K. Pretz, Smarter Sensors. The Institute, IEEE, pp. 6-7IOT sensors platform, March 2014.

[3] T. Karvinen, K. Karvinen, & V. valtokari, Make: Sensors, Maker Media Inc., Sebastopol, CA, May 2014

[4] www.adafruit.com

[5] www.memsic.com

[6] www.arduino.cc/en/Main/ArduinoXbeeShield

[7] CCTV cameras worldwide used in DDos attacks, www.zdnet.com/article/cctv-cameras-worldwide-used-in-ddos-attacks/, October 26, 2015.

[8] M. T. Dlamini, M. M. Eloff, and J. H. P. Eloff. Internet of things: emerging and future scenarios from an information security perspective. Southern Africa Telecommunication Networks and Applications Conference, 2009.

[9] C. Pfister, Getting started with the Internet of Things, O'Reilly, Sebastopol, CA, 2011

[10] J.P. Anderson, Computer security threat monitoring and surveillance. Retrieved September 23, 2011, from http://csrc.nist.gov/publications/history/, 1980.

[11] D.E. Denning, An intrusion-detection model. IEEE Transactions on Software Engineering, pp. 222-232, 1987

[12] T. F. Lunt, & R. A. Jagannathan, prototype real-time intrusion-detection expert system. IEEE Symposium on Security and Privacy, 59, 1988.

[13] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, & D. Wolber, A network security monitor. IEEE Symposium on Security and Privacy, 296, 1990.

[14] M. Weiser, The computer for the 21st Century, Scientific American, pp. 94-104, September 1991.

[15] V. Bharghavan, & C. V. Ramamoorthy, Security issues in mobile communication. Proceedings of the Second International Symposium on Autonomous Decentralized Systems, 19-24. 1995

[16] R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, M. A. Zissman, Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation. DARPA Information Survivability Conference and Exposition, 2, 2000.

[17] T. Bass, Intrusion detection systems and multisensor data fusion. Communications of the ACM, 43(4), 99-105. 2008

[18] W. Lee, & Y. Zhang, Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. 276-283, 2000.

[19] C. Iheagwara, A. Blyth, & M. Bennett, Architectural and functional issues in systems requirements specifications for wireless intrusion detection systems implementation. IEEE Systems Proceedings, 434 – 441, 2005.

[20] R. Roman, J. Zhou, & J. Lopez, Applying intrusion detection systems to wireless sensor networks. 3rd IEEE Consumer Communications and Networking Conference, 640-644, 2006

[21] I. Butun, S. D. Morgera and R. Sankar, A survey of intrusion detection systems in wireless sensor networks, IEEE Communications Surveys & Tutorials, 16(1), pp. 266-282, February 2013.

[22] Khune, R.S.; Thangakumar, J., A cloud-based intrusion detection system for Android smartphones, in Radar, Communication and Computing (ICRCC), 2012 International Conference on , vol., no., pp.180-184, 21-22 Dec. 2012

[23] N. Boggs, W. Wang, S. Mathur, B. Coskun, & C. Pincock, Discovery of emergent malicious campaigns in cellular networks. In Proceedings of the 29th Annual Computer Security Applications Conference, ACM, pp. 29-38, December 2013.

[24] G. Thamilarasu and R. Sridhar, CIDS: Cross-layer Intrusion Detection System for Mobile Ad hoc Networks, International Journal of Mobile Network Design and Innovation (IJMNDI), 2009

[25] H. Yang; J.-Hua Guo; Z. Zhong, On intrusion detection of RFID based on chaotic immune clustering model, in *Machine Learning and Cybernetics, 2009 International Conference on* , vol.1, no., pp.417-423, 12-15 July 2009

[26] G. Hao-yan; G. Chang-yong; W. Fa-Qiang, The design and realization of the integration of internet and LAN-based RFID and the intrusion detection system based on Snort in the RFID system with Ethernet interface, in *Aware Computing (ISAC), 2010 2nd International Symposium on* , vol., no., pp.181-184, 1-4 Nov. 2010

[27] L. Avanco, A. E. Guelfi, Elvis Pontes, A. Silva, S. T. Kofuji, and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. In RFID Technology (EURFID), 2015 International EURASIP Workshop on, pp. 73-80. IEEE, 2015.

[28] S. A. Shaikh, H. Chivers, P. Nobles, J. A. Clark, and H. Chen, A deployment value model for intrusion detection sensors, Lecture Notes in Computer Science in 3rd International Conference on Information Security and Assurance, vol. 5576., pp.250–259, June 2009.

[29] Z. Shelby and C. Bormann, 7LoWPAN: The Wireless embedded Internet, 1st ed.; John Wiley & Sons Ltd: Chichester, UK 2009.

[30] M.T.,Dlamini, M.M., Eloff, J.H.P., Eloff, Southern Africa Telecounication Networks and Applications Conference, Internet of things: emerging and future scenarios from an information security perspective, Aug 2009.

[31] L. Caiming, J. Yang, Y. Zhang, R. Chen, and J. Zeng. Research on immunity-based intrusion detection technology for the internet of things. In Natural Computation (ICNC), 2011 Seventh International Conference on, vol. 1, pp. 212-216. IEEE, 2011.

[32] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur, and A. Ingle. Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks. In Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on, pp. 1-7. IEEE, 2013.

[33] V. P. Kafle, Y. Fukushima, and H. Harai. Dynamic mobile sensor network platform for ID-based communication. In ITU Kaleidoscope Academic Conference: Living in a converged world-Impossible without standards?, Proceedings of the 2014, pp. 153-159. IEEE, 2014.

[34] C. Jun; C. Chi, Design of Complex Event-Processing IDS in Internet of Things, in Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on , vol., no., pp.226-229, Jan. 2014

[35] J. M., Batalla, P. Krawiec, Conception of ID layer performance at the network level for Internet of Things, Springer: Personal and Ubiquitous Computing V 18, pp. 465-480, Feb. 2014

[36] P. Kasinathan, C. Pastrone, M.A. Sprito, and M. Vinkovits. Denial-of-service detection in 6LoWPAN based Internet of Things. In 2013 IEEE 9th International onference on Woreless and Mobile Computing, Networking and Communications (WiMob'2013), Lyon, France, Oct. 2013.

[37] P. Kasinathan, G. Costamagna, H. Khaleel, and C. Pastrone, M. A. Spirto. DEMO: an IDS framework for Internet of Things empowered by 6LoWPAN. In 2013 ACM SIGSAC conference on computer & communications security1337-1340,November 2013.

[38] A. George, Popular Mechanics, How your world works, pp..21-22, December/January 2016.

[39] Travis Smith, Sweet Security Part 2 – Creating a Defensible Raspberry Pi http://www.tripwire.com/state-of-security/security-data-protection/sweet-security-part-2-creating-a-defensible-raspberry-pi/, January 2016.

[40] data.sparkfun.com