A SURVEY ON THE SECURITY OF IOT DEVICES

Waleed T. Al-Sit

Department of Computer Engineering, Mu'tah University, Al-Karak, Jordan
w_sitt@hotmail.com

ABSTRACT*—This review paper presents a survey of the different approaches to enhance the security of the Internet of Things Devices. The Internet of Things is a new concept where everyday devices are connected to the internet. This concept has widely spread during the very recent years. A problem came with the wide adoption of these devices, as these devices typically lack any kind of security measures or have insufficient security. In this pape, we discuss the different approaches to add security to the Internet of Things Devices.*

Keywords—Internet of Things; Security

I. INTRODUCTION

Internet of Things is a new concept that has been around for a few recent years, where everyday life devices are connected to the internet and can communicate with each other. This has led to the creation of new sensors which are also connected to the internet. Most of these devices come in the form of microcontrollers with limited computational power connected to both a sensor and a connection to the internet. Internet of Things devices is also typically running on a battery, resulting in a low power limitation. The problem with these devices is that they do not have any type of security measures in them, making hacking them a relatively simple task. Furthermore, these devices are plenty and relatively cheap, making them a great target to be compromised and used to execute distributed Denial of Service attacks or others as shown by [1]. Another aspect of worry with these devices is the possibilities of spying, identity theft, blackmailing, etc. Due to the above, work has been done on implementing security measures to protect these devices. This paper aims to assess their suggested techniques to tackle the problem.

The rest of the paper is discussed as follows. Section 2 shows the importance of secure Internet of Things devices. Section 3 discusses the important security aspects that need be covered for the Internet of Things applications. Section 4 discusses what work has been done in securing the Internet of Things devices. Finally, section 5 concludes the paper.

II. WHY INTERNET OF THINGS SECURITY IS AN IMPORTANT ISSUE

There are two aspects of Internet of Things devices which make them a highly valued target for malicious use [3]. First, due to the nature of their operation, they collect a lot of data.

If compromised this data can be seen by an attacker. Internet of Things devices are deployed in a lot of industries and residential homes due to their convenience. Hence, these devices could gather sensitive data that shouldn’t reach malicious hands. Secondly, is their widespread in sheer quantities. Internet of Things systems consists of a large number of small low power devices. That allows the easy and cheap deployment of these systems over larger areas. If compromised an attacker could use these Internet of Things devices to initiate a DDoS (Distributed Denial of Service) attack with relative ease, since they are already many internet connected devices in each Internet of Things system.

III. SECURITY ASPECTS IN NEED OF BEING COVERED

Internet of Things systems consists of three main elements. These elements are as follows:

Nodes or Sensor Units: Internet of Things Systems typically consists of many nodes or sensors. These are deployed to cover large and wide areas depending on the application to collect and transmit measured data. They could be directly connected to the internet or to a Base Station or Gateway. These devices typically communicate with each other or with the Base Station via wireless media. They are also usually battery powered. Therefore, these devices need to be operated in such a way so that they consume the least amount of energy possible. Any security measures on these devices have to be conscious of this power and energy limitation of these devices.

Base Station or Gateway: This element might not be always present on the Internet of Things systems. Usually, this element is used to gather data from the Sensor Units and might either send them as they are or organize them in a specific manner or might do some processing on them. These devices might not always be battery powered, it’s more often to find plug powered Base Stations than Sensor Units. Their existence in an Internet of Things system typically means they are the only connection between the Sensor Units and the World Wide Web or the internet. It’s might also be possible to configure the Internet of Things system using the Base Unit.

Wireless Communication Protocol: The Wireless Communication Protocol is the protocol used for communication in the Internet of Things system, between the Sensor Units themselves or if a Base Station is present then between the Sensor Units and the Base Station. The protocol has to be power and energy efficient in nature, as the Sensor Units don't have any energy or power to spare. It has to provide a wide range of coverage that is also relatively fast.

Each of these three elements must be designed with security in mind. None of the three elements must be compromised, otherwise, the entire Internet of Things system could be considered as if it's compromised as well.

There are three important aspects that need to be met to consider an Internet of Things system to be secure. These aspects are as follows:

Confidentiality means that the data stored anywhere in the Internet of Things system, typically in the base station, is not to be viewed by unauthorized users (either humans or machines). Only users with authority are allowed to view the data. Encryption or cryptography is the main technique to achieve confidentiality.

Integrity is about verifying that sent and received data has not been tampered with. Verifying that the data has actually been sent by the claimed author is also part of Data Integrity.

Authentication is about only allowing authorized users to access data gathered by the Internet of Things system, It’s also about confirming that there are no rouge or alien Sensor Units in the system and only allowing authorized Sensor Units to communicate with the Internet of Things system.

These three aspects of security have to be taken in consideration for applying security on the Internet of Things systems. Each of the three elements of the Internet of Things system has to be designed in such a way that it meets the requirements for Confidentiality, Integrity, and Authenticity.

IV. SOME OF THE PROPOSED SOLUTION TO SECURE INTERNET OF THINGS DEVICES

This section discusses various solutions tackling the issue of Internet of Things security:

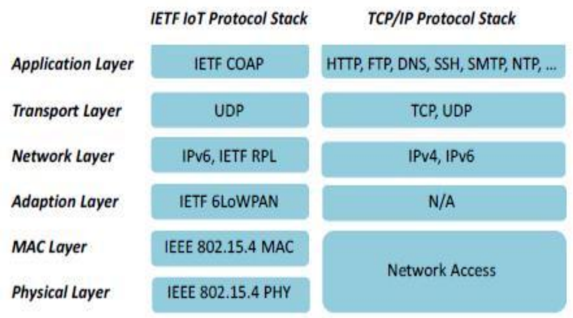
A. Relying on the existing Internet of Things protocol support

Reference [4] suggests a solution based on existing support for Internet of Things by the various network layers. Then it builds on it by proposing a gateway architecture solution

All internet protocols have been developed mostly for wall-powered devices, so they aren't optimized for low power applications. But since the Internet of Things devices have a hard power limitation, and sometimes energy limitations new protocols have been created to adhere to these low power requirements. Resulting in a full internet protocol stack for the Internet of Things. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN: RFC 6282) is an IPv6 protocol optimized for low power. There has been work to use this protocol for secure connections and encrypting data sent over the 6LoWPAN protocol [5,6]. For routing, the Internet Engineering Taskforce designed RPL [7] as a protocol that's suitable for low power networks, this protocol has been further enhanced in [8] producing Trust Anchor Interconnection Loop (TRAIL). TRAIL can prevent attacks from forged nodes by identifying and isolating them. For the application layer, CoAP [9] is suggested. CoAP is a stateless protocol that runs over the

User Datagram Protocol (UDP) for lower latency and faster connections. CoAP uses Datagram Transport Layer Security

[10] for security over UDP protocol. Figure 1. Shows how the resulting Internet Engineering Taskforce Internet of Things protocol stack compares to the traditional TCP/IP protocol stack.



	IETF IoT Protocol Stack	TCP/IP Protocol Stack
Application Layer	IETF COAP	HTTP, FTP, DNS, SSH, SMTP, NTP, ...
Transport Layer	UDP	TCP, UDP
Network Layer	IPv6, IETF RPL	IPv4, IPv6
Adaption Layer	IETF 6LoWPAN	N/A
MAC Layer	IEEE 802.15.4 MAC	Network Access
Physical Layer	IEEE 802.15.4 PHY	

Figure 1. The comparison between IETF IoT and TCPIP protocol stacks [4].

After laying a protocol ground suitable for a secure low powered application, the architecture comes next. The proposed solution is a gateway architecture. The gateway is a relatively powerful processor connected on the same network as the Internet of Things nodes, capable of managing them and providing interconnection between devices from different manufacturers. Two examples are mentioned. First, Integrated Access Gateway.

[11] tailored for home application. Second, a concept called Server-Based Internet-Of-Things Architecture (SBIOTA) [12], this gateway example also features auto-configuration so that minimal configuration is needed when being deployed. The author of [4] discusses two enhancements to be added to the architecture for sufficient security. These enhancements are 1) Gateway auto-configuration support and 2) Software and firmware updates for the Internet of Things devices. Figure 2 shows how the auto-configuration architecture works.

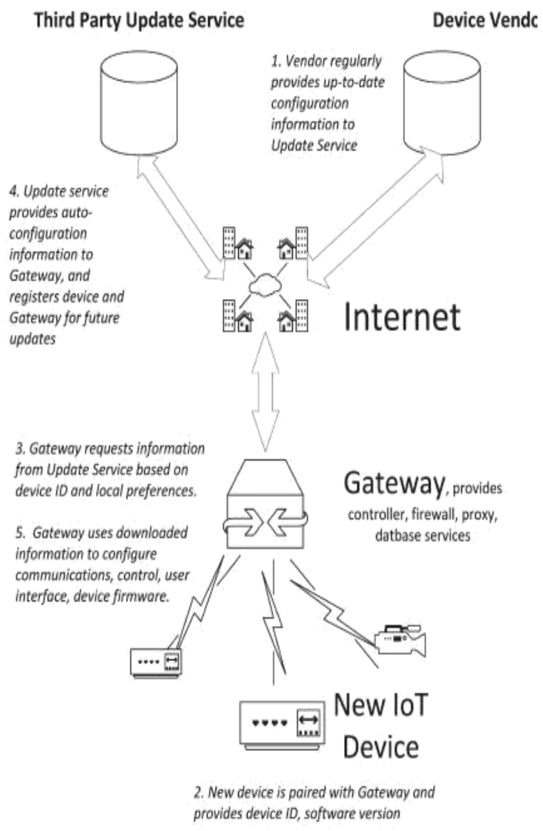

Third Party Update Service
Device Vendc
1. Vendor regularly provides up-to-date configuration information to Update Service
4. Update service provides auto-configuration information to Gateway, and registers device and Gateway for future updates
Internet
3. Gateway requests information from Update Service based on device ID and local preferences.
Gateway, provides controller, firewall, proxy, datbase services
5. Gateway uses downloaded information to configure communications, control, user interface, device firmware.
New IoT Device
2. New device is paired with Gateway and provides device ID, software version

Figure 2. Auto configuration architecture [4].

Security requirements for Internet of Things applications differ by the industry where it's used. In [4], the authors focus on the security for the Internet of Things for home applications. But that doesn't make them useless for other applications. Mission-critical applications, for example, are the different thing that needs their specific restrictions to be considered as well for their own security solutions. Most Internet of Things systems suffer from the necessity for manual configuration, that's where automation comes in handy, as it would make the Internet of Things systems secure without the intervention of the human users who purchase these products. Therefore, the need for automatic configuration as well as an auto update on these devices.

B. Securing sensor connections

The authors of [2] worked on a way to make a better connection to the Internet of Things sensors at the same time maintaining high-quality data in a continuous basis. As always, the problem is due to the low power restrictions of Internet of Things sensor nodes, leading to the use of low power, albeit low security, protocols. One such protocol is the basic LEACH routing protocol [15]. However, the basic LEACH routing protocol has many security vulnerabilities, making it possible for the Internet of Things systems using it to be abuse for Distributed Denial of Service attacks or their data could be compromised.

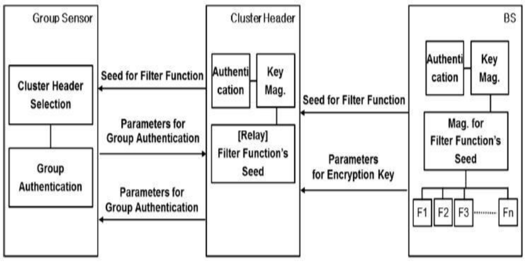


Figure 3. Concept of the proposed scheme [2]

Reference [2] proposes a comparable feature-wise protocol that is also secure. Figure 3 shows the concept of the proposed scheme. The proposed protocol only uses the four fundamental arithmetic operations as well as logical operations for authentication of nodes and secure data transmissions. The proposed protocol is secure against relay attacks, replay attacks, eavesdropping and leaked keys. It also supports sensor node anonymity, dynamic group management, mutual authentication, forward security, and error detection. With very low probability of successful outside attacks on the Internet of Things systems utilizing it. This probability was calculated to be 2*{1/(4*n-th Node)}^n.

The proposed protocol consumes around less than 8% more power compared to the basic LEACH routing protocol to meet the same performance. Figure 4 shows a graph plotting the critical distance between sensor node and base station versus energy consumption of the sensor nodes for the proposed scheme, the basic LEACH routing protocol and the LEACH-C routing protocol [16].

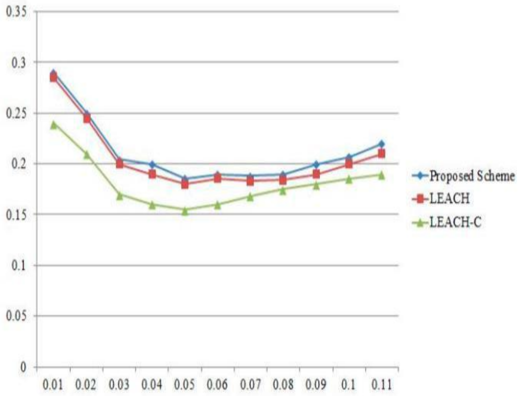


Figure 4. Performance analysis result [2]

For the performance analysis in Figure 3, the authors of [2] used randomly set sensors. Their environment size was 100 meters x 100 meters. A base station was located in a specific with consideration of their placement area. The distances between the randomly set nodes and the base station was within a range varying from 50 meters to 125 meters, depending on the specific placement of each set sensor nodes in the virtual environment. The test was set over various rounds each had a duration of 20 seconds. Those settings for the virtual test environment were configured in such a way so that they would be equivalent to the existing routing protocol environment.

As shown in Figure 4, the proposed scheme has a rather insignificant energy consumption increase over the basic LEACH routing protocol or the LEACH-C routing protocol. This slight energy consumption disadvantage is greatly outweighed by the proposed scheme's security advantage over the basic LEACH routing protocol and the LEACH-C routing protocol.

The proposed scheme in [2] supports mutual authentication between both the base station as well as the sensor nodes in an Internet of Things system environment. It also allows for confidential information transmission between the cluster headers that are dynamically allocated and groups.

C. Low energy encryption cipher

Low energy restriction is always a problem for the Internet of Things. The authors of [14] discuss two issues with 6LoWPAN:

(1) The lack of an efficient key generation mechanism; (2) It does not facilitate communication among many sensor nodes and it has a relatively short range. The suggested method of solving the first issue is to develop an energy efficient security algorithm based on an efficient key generation mechanism for secure data transmission. The suggested solution for the second issue is the use of the latest Wi-Fi standard which combines the advantages of Wi-Fi with low power communication. Reference [13] provides a detailed comparison between the latest 802.11 AH standard and the 802.15.4 standard. The 802.11 AH standard performs better compared to the 802.15.4 standard in terms of association time, delay, throughput, and coverage range. With the combination of low power Wi-Fi modules on the Sensor Units, it covers the low power restriction

For data security, in general, hash functions can be used or symmetric and asymmetric encryption algorithms. Due to the limited power available in the Sensor Units, the asymmetric algorithms are not suitable for the Internet of Things application. Hash functions and symmetric algorithms are then used for the security of the Internet of Things data. These include several famous ones like Message Digest 4 (MD4) [17], Message Digest 5 (MD5) [18], Secure Hash Algorithm 1 (SHA-1) [19], Hash Message Authentication Code (HMAC) [20], Data Encryption Standard (DES) [21], Advanced Encryption Standard (AES) [22], Rivest Cipher 4 (RC4) [23] and Blowfish [24]. But these algorithms were not created while keeping in mind the low power and energy constraint nature of the Internet of Things systems. Therefore, using them would not be ideal with the restrictions of electrical power, electrical energy, processor computational power, and low memory. Thus, the authors of [14] propose their own encryption algorithm which is optimized for the low resource restriction of Internet of Things Sensor Units. The Triangular Based Secure Algorithm (TBSA) is used as a potential solution for achieving energy efficient security for Internet of Things applications

TSBA was proposed to achieve confidentiality, privacy, integrity, and freshness of data with a realistic overhead relative to operation in an Internet of Things Sensor Unit. TBSA uses a much simpler key generation mechanism, as the block diagram in figure 5 shows. Therefore, it consumes considerably less power than typical hash functions and symmetric algorithms. It also saves power on data transmission between Sensor Units. The generated authentication key from the proposed key generation mechanism is then used to provide authentication between the elements of an Internet of Things system for data transmission. The proposed system attains three levels of authentication as show in figure 6.

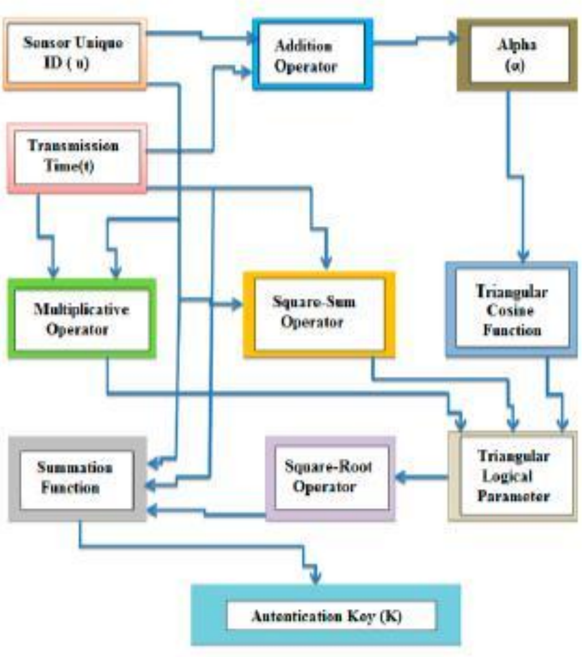


Figure 5. Key generation mechanism for the proposed TBSA [14].

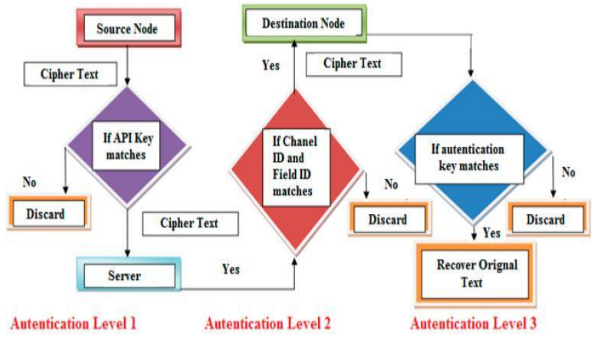
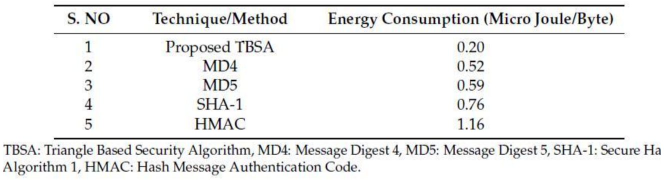


Figure 6. Three levels of network security for IoT based systems [14].

Reference [14] also shows energy measurements for TSBA compared to hash functions, symmetric algorithms, and other security mechanisms developed for Wireless Sensor Networks (WSN). Table 1 shows TBSA's energy consumption in comparison with hash functions. Table 2 shows TBSA's energy consumption in comparison with symmetric cipher algorithms. While figure 7 shows the same data in a column chart perspective. Table 3 shows TBSA's energy consumption in comparison with other mechanism developed for the use in WSN. While figure 8 represents the same data in a column chart perspective. The other mechanism developed for WSN which were compared against TBSA are PAWN a lightweight payload based mutual authentication method for cluster-based hierarchical WSN [27], PRESENT-GRP a novel hybrid lightweight security method for secure data transmission in Internet of Things based applications [26], and Alarm-Net an a system to monitor residential and assisted-living by query protocols [25].

Table 1. Energy consumption comparison with Hash functions [14].



S. NO	Technique/Method	Energy Consumption (Micro Joule/Byte)
1	Proposed TBSA	0.20
2	MD4	0.52
3	MD5	0.59
4	SHA-1	0.76
5	HMAC	1.16

TBSA: Triangle Based Security Algorithm, MD4: Message Digest 4, MD5: Message Digest 5, SHA-1: Secure Ha
Algorithm 1, HMAC: Hash Message Authentication Code.

Table 2. Energy consumption comparison with symmetric cipher algorithms from reference [14].

S. NO	Technique/Method	Energy Consumption (Micro Joule/Byte)

TBS/
Encr
ance

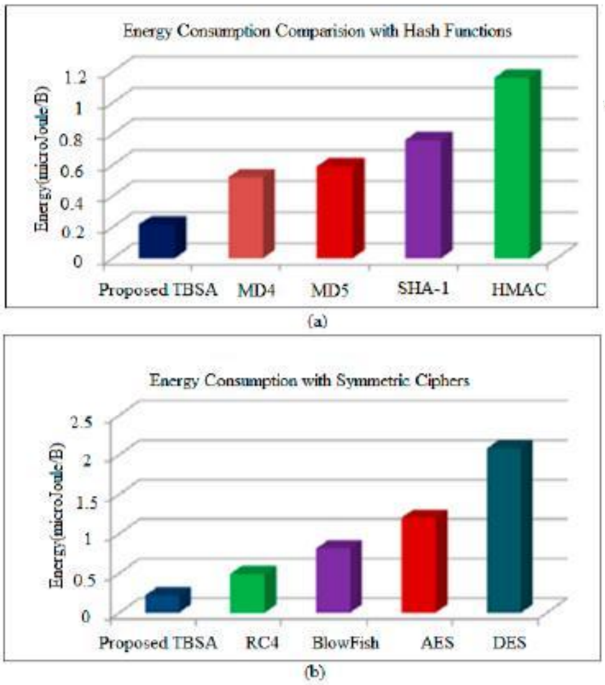


Figure 7. Energy consumption comparison of proposed TBSA (a) with Hash functions; (b) with a symmetric cipher algorithms [14].

Table 3. Energy consumption comparison with security methods designed for WSN from reference [14].

S. NO	Technique/Method	Energy Consumption (Micro Joule/Byte)
1	Proposed TBSA	0.20
2	PAWN	0.36
3	PRESENT-GRP	0.47
4	Alarm-Net	0.53

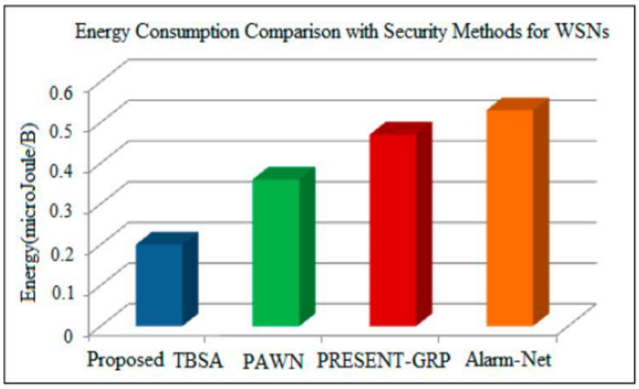


Figure 8. Energy comparison of proposed TBSA with security mechanics developed for WSN [14].

The energy measurement data provided in table 1, 2, and 3 and in figure 7 and 8 show that the proposed TBSA is superior to hash functions, symmetric cipher algorithms and other mechanisms developed for WSN security in terms of energy consumption in an Internet of Things environment while maintaining data security and authenticity.

D. Network-level security solution

The Authors of [28] propose a different way to enhance the security of the Internet of Things applications. Reference [28] proposes a similar take on security for IoT devices as to normal computer systems by inspecting the data in the network itself. But instead of using the common packet-based monitoring in the internet, they propose a lower cost flow-based monitoring.

They propose an architecture for flow-level characterization of IoT traffic that can detect malicious activity while minimizing the need to inspect packets. Which was validated experimentally by launching attacks on IoT devices? Their proposed architecture can achieve comparable security performance to packet-level inspection techniques at dramatically reduced costs. Figure 9. Shows their proposed test-bed.

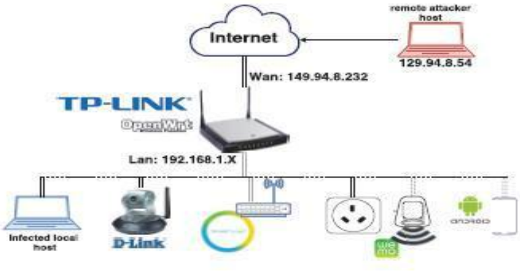


Figure 9. Proposed test-bed [28].

Figure 10. shows a pie chart that illustrates how cost-efficient the flow-level method is, causing an overhead of only 8% of the total data.

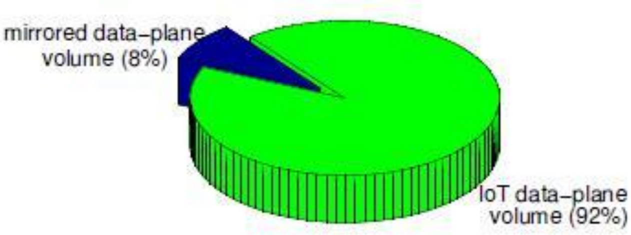


Figure 10. Total and overhead data volume.

V. Conclusion

Security for the Internet of Things systems is a very important issue, especially than every day more and more Internet of Things devices are being deployed in residential houses or in different industries. This rapid acceleration of insecure IoT devices would be a great target for attackers to do malicious deeds. Therefore, the security of these devices is of utmost

importance. Hence, a lot of research has been done in this area. Internet of Things consists of many elements, each needs its own security, and various research has been done on these different elements.

Authors in reference [4] rely on existing protocols designed for the Internet of Thins and low power applications. It's the reliance of 6LoWPAN might be considered a weak point considering 802.11 AH standards advantages over it with the combination of low power Wi-Fi modules. In reference [2] authors propose a routing protocol that is both low powered yet attains high-security levels. But might not be compatible with other systems. Others in reference [14] propose a highly energy efficient encryption algorithm that sits within the Internet of Things Sensor Units' various hardware limitations. While in [28], others refer mimics they widely used packet-level inspection and proposes a lower cost alternative with the same principles with the flow-level inspection. The results in [28] are comparable results to packet-level inspection but at a lower cost. Combining the proposed TBSA algorithm with other industry standards such as 802.11 AH and low power Wi-Fi modules provides a secure low power Internet of Things environment that is compatible with outside systems.

References

[1] J. Gondim, R. Albuquerque, A. Nascimento, L. Villalba, and Tai-Hoon

Kim “A Methodological Approach for Assessing Amplified Reflection Distributed Denial of Service on the Internet of Things” 2016

[2] Hyungjoo Kim and Jungho Kang “Dynamic Group Management Scheme for Sustainable and Secure Information Sensing in IoT” 2016

[3] Che Qiang, Guang-ri Quan, Bai Yu, and Liu Yang “Research on Security Issues of the Internet of Things” 2013

[4] Huichen Lin and Neil W. Bergmann. “IoT Privacy and Security

Challenges for Smart Home Environments” 2016

[5] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig,

"Securing Communication in 6lowpan with Compressed Ipsec" 2011

[6] Q. Yue and M. Maode, "An authentication and key establishment scheme to enhance security for m2m in 6lowpans" 2015

[7] A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.P. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" 2012

[8] H. Perrey, M. Landsmann, O. Ugus, T.C. Schmidt, M. Wahlisch, "Trail: Topology Authentication in RPL" 2013

[9] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (Coap)" 2014

[10] T. Dierks, and E. Rescorla, "The Transport Layer Security (Tls) Protocol Version 1.2" 2008

[11] F. Ding, A. Song, E. Tong, and J. Li, "A smart gateway architecture for improving efficiency of home network applications" 2016

[12] N.W. Bergmann, and P.J. Robinson, "Server-based internet of things architecture" 2012

[13] N. Ahmed, H. Rahman, M.I. Hussain "A comparison of 802.11 AH and 802.15. 4 for IoT" 2016

[14] Sandeep Pirbhulal, Heye Zhang, Md Eshrat E Alahi, Hemant Ghayvat, Subhas Chandra Mukhopadhyay, Yuan-Ting Zhang, and Wanqing Wu, "A Novel Secure IoT-Based Smart Home Automation System Using a
Wireless Sensor Network" 2016

[15] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan "Energy-Efficient Coomunication Protocol for Wireless Microsensor Networks" 2000

[16] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan "An application-specific protocol architecture for wireless microsensor networks" 2002

[17] H. Dobbertin, "Cryptanalysis of MD4". In Proceedings of the International Workshop on Fast Software Encryption, Cambridge, UK, 21–23 February 1996.

[18] J. Deepakumara, H.M. Heys, R. Venkatesan, "Fpga implementation of MD5 hash algorithm". In Proceedings of the Canadian Conference on Electrical and Computer Engineering, Toronto, ON, Canada, 13–16 May 2001.

[19] D.Zibin, Z. Ning, "Fpga implementation of SHA-1 algorithm". In

Proceedings of the 5th IEEE International Conference on ASIC, Beijing, China, 21–24 October 2003.

[20] M. Bellare, R. Canetti, H. Krawczyk, "Message authentication using hash functions: The HMAC construction". RSA Lab. CryptoBytes 1996, 2, 12–15.

[21] E.L. Horta, J.W. Lockwood, D.E. Taylor, D. Parlour, "Dynamic hardware plugins in an FPGA with partial run-time reconfiguration". In Proceedings of the 39th annual Design Automation Conference, New Orleans, LA, USA, 10–14 June 2002.

[22] A.K. Mandal, C. Parakash, A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES, Electrical". In Proceedings of the 2012 IEEE Students' Conference on Electronics and Computer Science (SCEECS), Bhopal, India, 1–2 March 2012.

[23] D. Chang, K.C. Gupta, M. Nandi, "RC4-hash: A new hash function based on RC4". In Proceedings of the International Conference on Cryptology, Kolkata, India, 11–13 December 2006.

[24] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)". In Proceedings of the International Workshop on Fast Software Encryption, Cambridge, UK, 9–11 December 1993.

[25] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, J. Stankovic, "Alarm-net: Wireless sensor networks for assisted-living and residential monitoring". Univ. Va. Comput. Sci. Dep. Tech.Rep.2006,2,1–14.

[26] D. Aakash, P. Shanthi, "Lightweight security algorithm for wireless node connected with IoT". Indian J. Sci. Technol. 2016, 9, 1–8

[27] J. Mian, N. Priyadarsi, U. Muhammad, H. Xiangjian, "PAWN: A payload-based mutual authentication scheme for wireless sensor networks". Concurr. Comput. Pract. Exp. 2016, 1, 1–10

[28] Sivanathan, Arunan, et al. "Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices." Proc. IEEE ANTS (2016).