PROPOSED LIGHTWEIGHT PROTOCOL FOR IOT AUTHENTICATION

Hiba A. Taresh1
[1]*Building and Construction Engineering Department, University of Technology, Baghdad, Iraq*
heba.art81@gmail.com

Abstract - The Internet of Things (IoT) alludes to interestingly identifiable items (things) which can communicate with different questions through the worldwide framework of remote/wired Internet. The correspondence system among an expansive number of asset obliged gadgets that produce substantial volumes of information affects the security and protection of the included items. In this paper, we propose a lightweight protocol for IoT authentication which based on two algorithms LA1 and RA1 which is used for authentication and generating session key that is used for encryption.

Keywords - IOT, Internet Of Things, Authentication Protocol

I. INTRODUCTION

During the last decade, the growth in the number of Internet enabled devices has been considerable. At the start of this expansion, people typically only owned a few Internet capable devices, typically in the form of personal computers. Today more and more devices have interfaces that allow Internet connectivity. One of the most significant developments has been in the number of smart phone devices. Currently people frequently own many devices that they use interchangeably for Internet access. Every day additional devices join the global Internet, potentially permitting access to or from them by other Internet enabled devices. The term Internet of Things (IoT) was proposed by K. Ashton during the year of 1999 [2], although the concept was discussed in scientific literature prior to this time. This term tries to define a future Internet where the growth in the number of device continues and almost all electronic devices have Internet connectivity. This growth is not limited to usercontrolled devices, but also includes machine to machine (M2M) communication, such as smart sensor systems. All of these Internets connected devices will have a representation in the Internet either in the form of an IP address or some other identifying information. Setting up such an infrastructure has many benefits, including remote monitoring, convenient control of devices owned by an individual and increasing numbers of automated systems. Estimates of the number of wireless devices connected to the
Internet suggest 30 billion devices by 2020 [3]. Even today, IoT has emerged as an area for research and development. A "constrained device" is a device that has limited number of resources according to processing capacity, memory, or available power. Constrained devices are often used to implement sensor networks and automated systems that utilize M2M communication. The reason these devices are used is that they are small, inexpensive, and can perform the desired function(s), while consuming very little power. The software running on these devices has to be adapted to this constrained environment and ensures sufficient performance without requiring high speed processing, large memory capacity, or using excessive power [4]. Creating small IP stacks and similar software have been necessary steps to realize IoT and to allow constrained devices to communicate efficiently via a network [5]. Making IoT devices accessible through the same protocols used in the global Internet is also important when interconnecting these devices to the existing network infrastructures [6]. Security is another important aspect of the IoT. If all devices have an IP-address and are accessible via the Internet, then security becomes an even more important issue as the number of potential attackers is greatly increased. Authentication is vital to prevent certain types of attacks against these devices and to confirm the validity of messages [7]. For instance, a device can be inundated with messages in order to exhaust its battery supply, thus authentication has to be performed in an efficient manner and properly take into
Iraqi Journal for Computers and Informatics (IJCI) Published by University of Information Technology and Communications (UOITC)
account the device's limited power, storage, and computing capabilities[8]. Because of this, the protocols used for authentication have to be adapted for these constrained devices and must meet requirements beyond the conventional requirements for mains powered devices [9]. Combining the fast growth of IoT devices with limited resources and less mature security options means that these constrained devices can become a prime target for attacks [6]. If these issues are overlooked, then sensitive systems including devices controlling people's homes or industrial applications are at risk [10]. This is especially true if devices such as smart light bulbs, industrial sensors, radiators, and other such applications continue to gain in popularity [3]. It is important that security is built into the IoT as early as possible, as retrofitting security solutions is more a difficult challenge [11].

A. THEORETICAL BACKGROUND:

1. Internet of Things (IoT) Technology: Set This term portrays a few innovations and study teaches which empower the Internet for connecting to this present reality of physical articles. Advancements such as RFID, short-extend remote interchanges, ongoing limitation, and sensor system IoT device

are ending up progressively inescapable, turning IoT to reality [12].

2. Communication

The following communication technologies represent the main technologies used in IoT:

1-Satellite [13]: Cell - 4G/LTE, 3G/GRPS, 2G/IOT NETWORKEDGE,CDMA,EVDO GPS - Global Positioning System IOT NETWORK - (GSM communications) is an open, computerized cell innovation which is used to transmit versatile voice and data administration.

2-Tower [14]:

Weightless - it is a suggested exclusive open remote innovation standard for trading information between a base station and a great many devices that surround it utilizing White space (i.e. wave-length radio transmission in empty TV transfer channels) with abnormal amounts of security. Range: Up to 10km

WIMAX -is a remote interchanges standard intended to give between (30 and 40) mbit/s data rates,[1] with the 2011 refresh giving up to 1 Gigabit per second [1] for settled
stations. The discussion depicts WiMAX as "measures based innovation empowering the conveyance of last mile remote broadband access as another option to link and DSL". Range: Up to 50km

DASH 7 - an open source RFID-standard for remote sensor organizing that operates in the 433 MHz unlicensed ISM band/SRD band. DASH7 provides multi-year battery life, range of nearly 2 Kilometers, indoor scope with 1 m. accuracy, low inertness for interfacing with things in motion, a little open source convention stack, AES 128-piece shared key encryption support, and information exchanging of about 200 kilo-bit per second. DASH7 refers to the innovation that has been found by the non-profit organization known as the “DASH7 Alliance”. Range: up to 2km

3-Wireless Access Point: WiFi - Wi-Fi is an innovation that enables an electronic gadget to trade information remotely (utilizing radio waves) over a PC organize, including rapid Internet associations. The Wi-Fi Alliance defines Wi-Fi as any "remote neighborhood" (WLAN) item IoT device depending on the “Institute of Electrical and Electronics Engineers” (IEEE) 802.11a/b/g/n/af

Range: typical range is about 100 meters however could be expanded. Bluetooth - a remote innovation standard to trade data over short separations (with the use of short-wavelength radio transmissions in the ISM band between (2400 MHz and 2480 MHz) from settled and cell operations, producing individual zone system IoT device (PANs) with large amounts of security [15]. Range: 1-100m

Bluetooth Low Energy - Bluetooth low vitality remote, on account of its inventive plan, expends just a small amount of the energy of Classic Bluetooth radios. Bluetooth low vitality innovation broadens the utilization of Bluetooth remote innovation to gadgets that are fueled by little, coin-cell batteries, for example, watches and toys. Different gadgets, for example, sports and wellness, medicinal services, human interface (HIDs) like consoles and mice and amusement gadgets will likewise be improved by this form of the innovation. Much of the time, it makes it conceivable to work these gadgets for over a year without reviving. DIHilarly as with past adaptations of the determination, the scope of the Bluetooth version 4.0 radio might be enhanced by application. The greater part of Bluetooth gadgets which are common recently include the fundamental 30 foot, or 10m, range of the Classic Bluetooth radio, yet there isn’t any restrictions forced by the Specification. With Bluetooth v4.0, producers may enhance range to about 200 feet and past, especially for domestic sensor implementations in which longer range is a need. Bluetooth low vitality remote innovation, the trademark highlight of the v4.0 Bluetooth Core Specification, Range: 1-100m

RFID - ISO RFID Complete rundown of gauges a radiorecurrence distinguishing proof model uses labels, or names connected to the item IoT device to be recognized. Two-way radio transmitter-beneficiaries known as investigative specialists or perdevice s send a flag to the tag and then waits for its reaction. The perdevice s usually transfer their perceptions to a PC model that runs RFID programming or RFID middleware. RFID labels could be inactive, dynamic or battery aided uninvolved. A dynamical tag has an onboard battery and discontinuously transfers its ID flag. A battery aided inactive (BAP) has a small battery on board and it is initiated when within the sight of an RFID for each device [16].
Range: 10cm to 200m

NFC - Near field correspondence is an arrangement of shortrun remote advances, regularly require a separation of 10 centimeters or less. NFC works at 13.56 MHz on ISO/IEC 18000-3 air interface and at rates extending from 106 kbit/s to 424 kbit/s. NFC dependably includes an initiator and an objective; the initiator effectively produces a RF field which can control an inactive target. This empowers NFC focuses to take extremely basic shape factors, for example, labels, stickers, scratch coxcombs, or cards which don't need batteries. NFC distributed correspondence is conceivable, given the two gadgets are fueled [17]
Range: < 0.2 m

II. PROPOSED LIGHTWEIGHT PROTOCOL:

In this work a new proposed protocol for authentication in IoT is proposed based on figure (1) architecture two algorithm are proposed inside this protocol (LA1 algorithm) for verification and authentication between the device and the IoT network, (RA1 algorithm) for generating secure key for encryption (session encryption key) which used for
encrypting the data by proper encryption method the device should be authenticated to connect to the IoT net-work and for connecting to the cloud network and send the data encryption operation should be applied the encryption key is calculated mutually between the IoT device and the network.

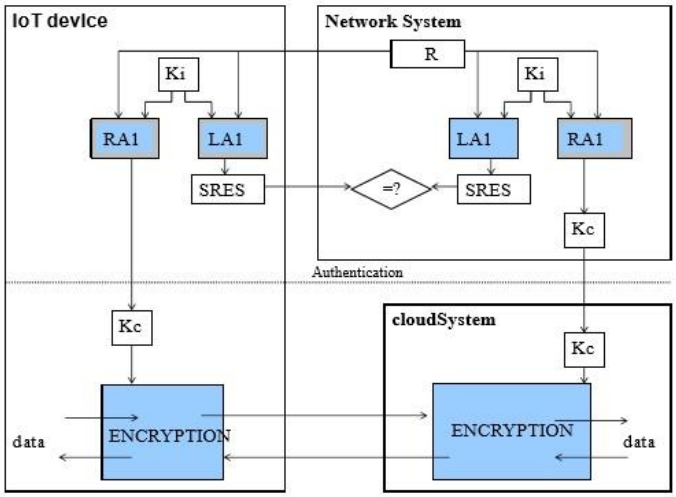

Fig. 1: The proposed authentication protocol architecture

A. Device Identity Holder (DIH)

The DIH (Device Identity Holder) is a smart card need to be integrated to the device s connected to the IoT Networks. Because it is a smart card, some inherent security functions are included in it that is specified to smart cards. It has several security attributes owned by the operating system and chip hardware in smart card. Device Identity Holder includes the required data that helps accessing the device account. Ki and GIDN are generally preserved in every DIH. GIDN (Global IoT Device Number) usually comes with 15 digits (at most) devoted uniquely to the entire mobile device all over the world. Individual device authentication Key (Ki) is a random number (128-bit), the session key generator, is considered as the origin cryptographic to provide these keys and provides the authentication of the device with the network. Individual device authentication Key (Ki) is protected severely and stored in the device's DIH .The DIH is itself protected. Secrecy of Ki and GIDN are in charge of Confidentiality and Authentication of device data. With discovering of these numbers, anyone can impersonate a legitimate device. In every DIH (LA1 and RA1) algorithm IoT device are also implemented. This helps the operator to change and determine this algorithm IoT device independently from hardware manufacturers and the other operators. Therefore, authentication works when a device is peregrination on other Network. LA1 is used mainly for device s authenticating to the network but RA1 is used for (Kc) session key generating. Random challenge sends by network to the device so Kc and SRES are produced by DIH. When device authenticated, the net-work order the operation for starting the encryption process via utilizing the generated (Kc) session key.

B. Authentication in IoT

The IoT network blends specific security services for devices and for IoT cloud network as well. These networks always will do the following:

• Verify the identity of device, authentication of IoT is responsible for it (LA1 algorithm).

• Keeping the identity secret, anonymity is very important to devices.

• Using proposed number GIDN (global IoT device number) identifies the device s equipments.

• Using DIH (device identity holder) for keep track of device identity and location.

C. Devices Identity Authentication: The DIH card holds operation number, authentication key Ki, GIDN, device relevant data and security algorithm IoT device such as authentication algorithm (LA1). The NDLR (Network devices location register) stores also a copy of Ki and GIDN and so on. In IoT Network, after the devices are recognized and passed authentication then services can be provided. The authentication protocol in IoT network is made up of a (challenge-response principle). It depends on using a (private key) Ki that is sharable between IoT device and NDLR. When IoT device request free channel by making request with network, it requests for an update of its location to IoT device (network devices location register). The IoT network, as response, asks IoT device for its authentication.

D. Authentication using LA1 Algorithm

IoT Network works like any other network so it requires authentication in network security, LA1 will check if the current communication is authentic. Unauthorized device will be prohibited from logging in the network claiming to be confided device. LA1 faces many types of challenge between the network and the IoT device, the IoT device should respond to them completely and correctly. If all fails, it will prohibit connecting to the network, Figure (2) describe how the LA1 algorithm works. Algorithm (1) illustrates the LA1 authentication algorithm.

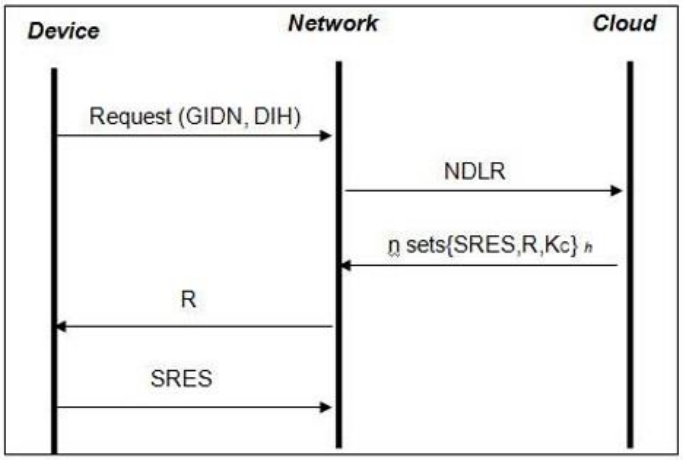

Fig.2: LA1 algorithm

Algorithm1 LA1 authentication Algorithm
Input: RAND (128 bit), Ki (128bit). Output: 32 bit
Process: Step1: Ki is provided to network by IoT device.

Step2: A 128-bit random number is generated by the network (RAND) by the Network devices location register (NDLR).
Step3: LA1 generates authentication sign (SRES), 32 bit is generated by IOT DEVICE and mobile services switching centre and it is signed response.
Step4: RAND is sent to operation by network.
Step5: If the two values of SRES are equal Authentication is successful, device can join the network go to step 6. Else the device prohibits entering the network.
Step6: End.

E. Key Generating Algorithm in RA1:

Device data and signal data need to protect from interception by encryption. Generally Symmetric cryptography used by the IoT network system. In symmetric cryptography encryption algorithm and encryption key are needed. In IoT network IoT device, the encryption key (Kc) is 64-bit and used as a Session Key for encryption, IoT device generates Kc by using (RAND) from the IoT network and the (Ki) from the DIH by using the RA1 algorithm.
Algorithm (2) illustrates the RA1 algorithm.

Algorithm2 RA1 Confidentiality Algorithm
Input: RAND (128 bit), Ki (128bit). Output: 64-bit encryption key.
Process: Step1: Ki is provided to network by IoT device. Step2: A 128-bit random number is generated by the network (RAND) by the Network devices location register (NDLR). Step3:RA1 generates Session Key (Kc) of 64 bits used in encryption. Step4: IoT device (IoT device) sends the Session Key (Kc) to the IoT network Step5: Kc is then stored in the DIH and readable by the operation. Step6: The network also generates the Kc and distributes it to the IoT network handling the connection. Step7: End

F. Comparison in IOT authentication:

Mobile nodes in IoT frequently move from one cluster to another, in which cryptography based protocols are used to allow expeditious identification, authentication, and privacy protection. This protocol also accommodates a valid demand message

TABLE (1): CONTRIBUTION OF ONGOING EUROPEAN PROJECTS ON IOT SECURITY

IOT Security	Project Names: Butler [17]	EBBITS [18]	Hydra [19]	uTRUSTit [20]	iCore [21]	HACMS [22]	NSF [23]	FIRE [24,25]	EUJapan [26]	proposed
Access Control	✓	✓		✓	✓	✓	✓	✓		✓
Privacy	✓				✓		✓	✓	✓	✓
Enforcement										✓
Trust					✓		✓			✓
Mobile	✓			✓			✓			✓
Middleware		✓	✓		✓					✓
Confidentiality	✓	✓	✓		✓	✓	✓	✓	✓	✓
Authentication	✓			✓	✓	✓	✓	✓		✓

and an answer authentication message, which speedily implements identification, authentication, and privacy protection. It will be useful to safeguard against replay attack, eavesdropping, and tracking or location privacy attacks. In contrast with other similar protocols such as basic hash protocol, it has less communication overhead, more secure and provides more privacy protection. Summarizing, also if the security issues of mobile devices (i.e., devices identification and authentication, key and credential storage and exchange) are under investigation by the scientific community, the available solutions partially
address these needs, thus requiring further efforts in order to allow the integration with the other IoT technologies.

III. CONCLUSIONS:

The Internet of Things (IoT) will lead to connect the things together via the cloud and internet these devices need to be authenticated before connecting to the network in this paper we introduce a proposed light weight protocol to achieve this goal.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IOT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[2] R. Want and S. Dustdar, "Activating the internet of things [guest editors'introduction]," Computer, vol. 48, no. 9, pp. 16–20, 2015.
[3] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major,and L. Kerr, "Security in the industrial internet of things," 2016.
[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: areview," in Computer Science and Electronics Engineering (ICCSEE),2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.
[5] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner,"Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472.
[6] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198– 213, 2016.

[7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[8] L. Da Xu, "Enterprise systems: state-of-the-art and future trends," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.
[9] P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.
[10]Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things," Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.
[11]Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.
[12]S. Misra, M. Maheswaran, and S. Hashmi, "Security challenges and approaches in internet of things," 2016.
[13]M. C. Domingo, "An overview of the internet of things for people with disabilities," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.
[14]W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologies of internet of things perceiving mine," Procedia Engineering, vol. 26, pp. 2326–2333, 2011.
[15]H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," in Internet of Things. Springer, 2012, pp. 572–580.
[16]B. Karakostas, "A dns architecture for the internet of things: A case study in transport logistics," Procedia Computer Science, vol. 19, pp. 594–601, 2013.
[17]H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of security services for resource constrained internet of things," International Journal of Distributed Sensor Networks, vol. 2016, 2016.
[18]S. Khan, M. Ebrahim, and K. A. Khan, "Performance evaluation of secure force symmetric key algorithm," 2015.
[19]] P. L. L. P. Pan Wang, Professor Sohail Chaudhry, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337–359, 2016.
[20]M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer 2 peer system; an approach towards surmounting security challenges," arXiv preprint arXiv:1404.5123, 2014.
[21]M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," Computer Communications, 2016.
[22]L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[23] F. Xie and H. Chen, "An efficient and robust data integrity verification algorithm based on context sensitive," way, vol. 10, no. 4, 2016.
[24]S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.
[25]T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (rfid) systems," NIST Special publication, vol. 80, pp. 1–154, 2007.
[26]J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil attack detection based on rssi for wireless sensor network," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2684–2687.
[27]S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the sybil attack cooperatively in wireless sensor networks," in Computational Intelligence and Security, 2008. CIS'08. International Conference on, vol. 1. IEEE, 2008, pp. 442–446.
[28]Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418–2434, 2010.
[29]S. Chen, G. Yang, and S. Chen, "A security routing mechanism against sybil attack for wireless sensor networks," in Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 142–146.
[30]L. Eschenauer and V. D. Gligor, "A keymanagement scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 41–47.