2014

Securing the internet of things infrastructure – standards and techniques

Zubair A. Baig
Edith Cowan University

DOI: 10.4225/75/57b6651c343d6

12th Australian Information Security Management Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

SECURING THE INTERNET OF THINGS INFRASTRUCTURE – STANDARDS AND TECHNIQUES

Zubair A. Baig
Security Research Institute & School of Computer and Security Science
Edith Cowan University, Perth, Australia
z.baig@ecu.edu.au

Abstract

The Internet of Things (IoT) infrastructure is a conglomerate of electronic devices interconnected through the Internet, with the purpose of providing prompt and effective service to end-users. Applications running on an IoT infrastructure generally handle sensitive information such as a patient's healthcare record, the position of a logistic vehicle, or the temperature readings obtained through wireless sensor nodes deployed in a bushland. The protection of such information from unlawful disclosure, tampering or modification, as well as the unscathed presence of IoT devices, in adversarial environments, is of prime concern. In this paper, a descriptive analysis of the security of standards and technologies for protecting the IoT communication channel from adversarial threats is provided. In addition, two paradigms for securing the IoT infrastructure, namely, common key based and paired key based, are proposed.

Keywords
Internet of Things (IoT), End-to-end security, Resource-constrained devices

INTRODUCTION

Internet-of-things (IoT) has emerged as a term to aptly describe the end-to-end platform for sustaining a device-to-Internet-to-device communication model. These large set of electronic devices form the core of an IoT infrastructure, to support every day user activity for a plethora of applications. The evolution of the Internet, attributed primarily to advances in communication bandwidth accompanied with rapid development of diverse user-specific applications, has sustained a progressive march towards introduction of efficient electronic devices to facilitate our daily activity. These set of devices constituting an IoT architecture are tiny (can generally fit into a consumer's pocket with ease), and exhibit features that help facilitate smooth and convenient user/business-activity on the go. Some of these devices include RFID tags, wireless sensors and mobile phones. Through the IoT infrastructure, end-users control applications required for: remote transmission of emails, blood pressure monitoring and transmission to a remote healthcare facility and remote transmission of the geographical position of a truck carrying goods to its destination.

Moreover, rapid advances in processing and communication capabilities of these small devices over the last decade, has made communication over longer distances with imposed real-time constraints, realisable. The interaction of these IoT devices with legacy systems requires efficient and secure usage of the Internet communication infrastructure. As a result, not only can IoT devices establish and use remote communication to convey a status report of a particular event or activity, but can also provide end-users with a higher level of confidence in the privacy and authenticity of all services provided therein. The level and procedure to provide privacy and security to an IoT infrastructure will vary in diversity, description, as well as complexity, depending upon the IoT devices in use. For instance, a mobile phone connected through a 3G communication channel to the Internet will implement a different set of protocols for securing the channel, as opposed to a resource-constrained RFID tag, that will invariably have a customised version of a resource-demanding secret-key verifier.

In Fig. 1, the IoT infrastructure consisting of a set of heterogeneous IoT devices along with their respective communication channels is illustrated.

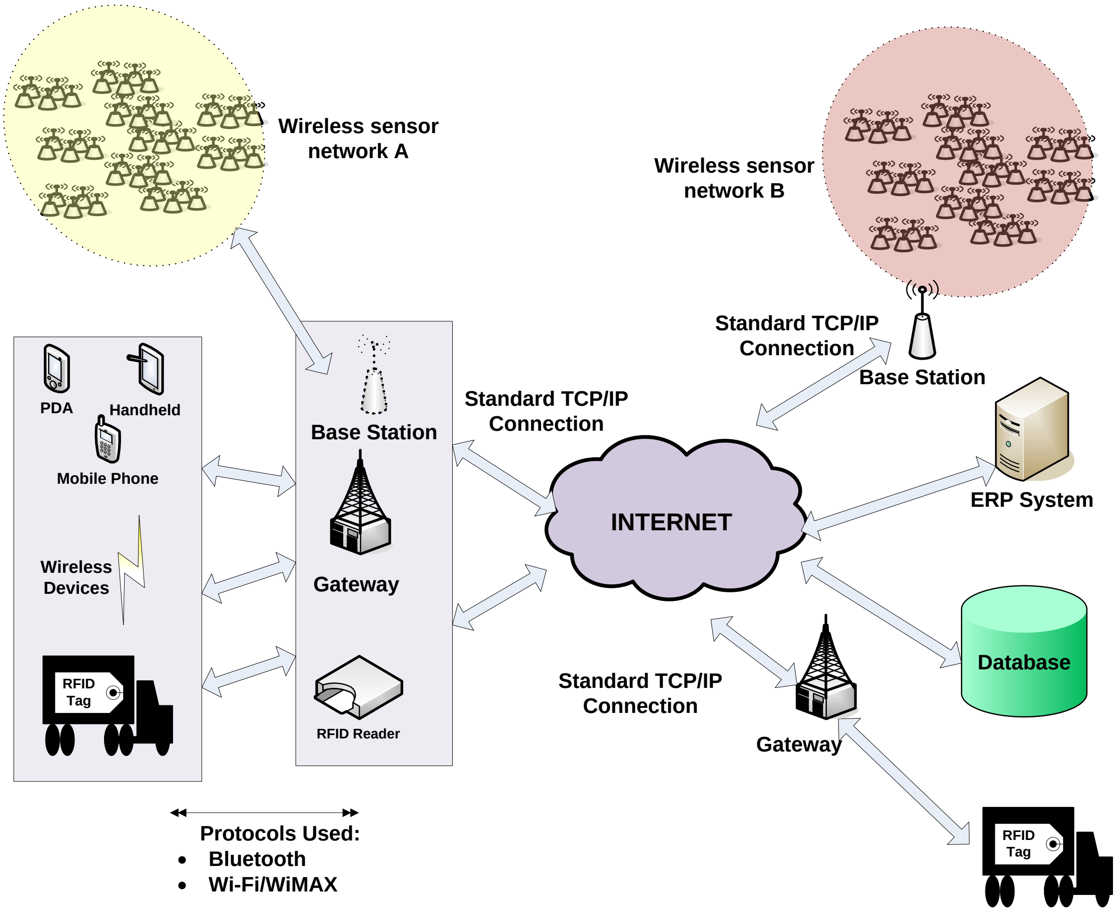


Figure 1.The IoT network infrastructure with an illustration of the standards/protocols used.

SECURITY FOR WIRELESS SENSOR NETWORKS

A Wireless Sensor Network (WSN) is defined as a collection of resource-constrained devices called sensor nodes reporting their individual readings in the form of sensory data to a high-performance base station (Masayuki et al., 2006). Under the context of the IoT infrastructure, such networks will serve several applications such as environmental monitoring, structural health monitoring, security, reconnaissance, and early warning applications. WSN nodes have an on-board processor (such as an ATMEGA 128-bit microcontroller), wireless communication capability (such as 802.15.4), a sensing module, and memory (around 128 KB of Flash and 8KB of RAM) (Rutlidge, 2008). The gateway is responsible for managing, coordinating, and scheduling operations of sensor nodes. Contemporary sensor nodes are capable of providing Advanced Encryption Standard (AES)-based encryption and decryption of the communication channel between the node and its gateway. Considering the limited radio range of sensor nodes, the gateway must be located within close proximity of the sensor nodes so as to reduce the overhead associated with wireless transmissions over longer distances.

Some of the most common attacks against wireless sensor networks, as may also be present in other networks, exploit vulnerabilities that may fall under one of the four security threat categories. Eavesdropping of sensory data, transmitted from a sensor node to its base station is a very common threat in these networks. The purpose of such an activity is to unlawfully access sensitive data associated with a particular event or phenomenon in nature. For instance, the geophysical location of a truck carrying goods from one logistic location to another, upon disclosure may provide unfair advantage to competitors. Privacy of all sensor network communication can be achieved through the use of a secret-key based mechanism, wherein all sensor node-base station pairs will possess a shared secret key. In such a scenario, all data transmitted from a sender to the receiver needs to be encrypted using symmetric key encryption based on a standard algorithm such as AES, and subsequently decrypted at the receiver's end using the same shared key.

An alternative to the above scheme is to use public key cryptography, wherein each sensor node as well as the base station will possess a pair of keys, namely, *public* and *private*, for data encryption and decryption. Such a scheme will demand greater processing power to support operations such as modular exponentiation of large prime numbers. As a result, tiny sensor nodes will suffer from rapid consumption of battery life. Advances in processing technology, accompanied with the potential to harness the availability of renewable sources of energy such as solar power, are alleviating concerns associated with sensor battery life in contemporary times.

The integrity of sensory data may be affected due to the presence of an adversary in close vicinity of a sensor network. The adversary may tamper with sensory data with the purpose of misleading information stakeholders, connected to a base station, in effect causing losses (possibly catastrophic in nature). For instance, a network of sensors deployed to monitor a bush fire, if compromised, may generate incorrect readings to deceive the base station, by portraying *normal* environmental conditions. In addition, an adversary may also inject malicious data into the sensor-to-base station communication channel, again with mal intentions. An effective approach towards verification of message origin and integrity is to use message authentication codes (MACs). A MAC is a hash of a simple concatenation of the message to be transmitted with a secret key shared between the sender and the receiver. A standard hash function such as MD-5 or SHA-1 would serve the purpose. A message is thus appended with the MAC, and sent to the destination, where the MAC of the received message is recomputed and compared with the received MAC, for verification.

A message appended with the current time of the day or a fresh nonce (random number) before transmission, will also prevent a replay attack, wherein a stale message is replayed by the adversary, again to mislead information stakeholders, such as firefighters, awaiting advice from the base station.

Jamming attacks (Sun et al., 2007) are launched by an adversary to incapacitate the sensor to base station communication channel from carrying signals. A jammer generates collisions on the communication channel in order to disrupt routine message communication. The purpose of such an attack is primarily sabotage, wherein the attacker attempts to prevent the base station from receiving actual readings from the sensor network. For instance, the blood pressure of a hypertensive patient may be prevented from being transmitted to the nearest base station, for subsequent rendering to a remote healthcare facility. A common practice in thwarting jamming attacks is to use random time slots for transmission of data, and random frequency hopping, so as to keep the attacker guessing, and to prevent it from disrupting signals.

RFID TAG SECURITY

A passive RFID tag has no processing power, but rather stores the ID of the tag in a particular format such as a barcode, readable by an RFID reader. Active RFID tags are battery-powered, and can read from a distance of up to hundred feet, and are therefore more versatile as compared to their passive counterparts. However, RFID tags operate at 100 Khz with on-chip RAM of 8Kbytes (Abe et al., 2006). Such limited resources are generally insufficient to hold and process large exponents required for public key cryptography.

The primary concern in providing security to RFID devices is the scarcity of computational and communication resources available on the device. Moreover, RFID tags do not have enough on-chip real-estate to accommodate large numbers of logic gates, necessary for real-time computation of complex key generation/verification activity. For instance, a typical public key-based encryption using NtruCrypt on an RFID tag will require the processing capability of 3000 logic gates, and will use a large portion of the available tag battery (if it is an active tag), or will incur a long delay in acquiring power passively from an RFID reader. It may also be worth noting that an encumbered usage model of these devices will affect their marketability, and in effect cause the technology to lose pace of growth.

Apart from encryption of all RFID tag data, authenticity of the tag itself is of utmost concern, to ensure uniqueness of user identity and thus secure access to other resources such as RFID readers. RFID tags may possess a unique collection of identifiers known as pseudonyms, which may be used on a rotating basis by the tag (Juels, 2006). An authorised tag reader, subject to a priori correspondence with the tag for exchange of pseudonyms, can identify these tags without much hassle. A possible malicious attack against such a scheme may involve the eavesdropping of RFID-to-RFID tag reader communication, over a period of time, to reconstruct the entire pseudonym set from a given tag, for possible reuse by the attacker, at a later stage. Data encryption through the use of either public-private key pairs or through symmetric keys will help counter the threat. However, the limit on the key lengths for due sustenance of cryptographic operations on RFID resources, exposes such devices to dictionary and brute-force attacks.

MOBILE DEVICE SECURITY

Mobile devices such as phones and personal digital assistants (PDAs) have become the present-day norm for information sharing and communication. The security of such devices can be categorised into two – social and technology-dependant. A mobile device is only as secure as the perception of its owner. Most mobile devices do not have a passkey lock, and generally hold plaintext information. Such information may include private telephone numbers, bank account details (of less-careful users), and other personal information such as messages. A phone handed over heedlessly by its owner to another user, will have all its information exposed. A mobile device may also be utilised for providing real-time video footage of a patient in need of remote monitoring and health tips, to possibly recover from a health hazard. Such information is sensitive, and may also prove to be catastrophic to the patient, if compromised or tampered with, by an adversary. However, to preclude such incidents from taking place, the communication channel standards used for mobile communications such as the Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA), have in-built mechanisms for data encryption and device authentication.

The GSM service provides stream cipher support for encrypting all data that is communicated between a subscriber and a service provider (mostly a gateway). Some of the encryption techniques such as the A5/1 cipher of the GSM service have been hacked, using *known plaintext attacks*, wherein an attacker generates a large set of plaintext messages, and uses the encryption algorithm to encrypt these messages (Bouska and Drahansky, 2008). A large set of these plaintext message-ciphertext pairs will help the attacker construe the secret key, or to accurately guess the encryption algorithm, by mere observation of a pattern in the collected data.

BLUETOOTH SECURITY

Bluetooth is a wireless technology standard for facilitating exchange of data over short distances. Bluetooth technology provides for security at the link layer, to support key management, user authentication, and data encryption (Yan et al., 2008). For any two Bluetooth-enabled devices to communicate securely, a pairing procedure is carried out before actual communication begins. Earlier versions of Bluetooth (< v2.1) required each device to enter the same PIN code on a device keypad, to successfully establish a connection. These devices were therefore hardcoded with fixed PINs such as ‘1234’ to establish an inter-device connection without user intervention. Devices enabled with Bluetooth v2.1 and above use the Secure Simple Pairing (SSP) procedure, which is secured through PKI. One of four pairing procedures may be used for this purpose: a) *Security mode 1*, as such no user interaction is enforced, and a device automatically generates a PIN based on factory-level specifications, and establishes communication with another Bluetooth device in the vicinity. Head-sets are generally reliant on this mode, b) *Security mode 2*, a numeric comparison of PIN codes entered by the users on the keypads of two devices that wish to communicate with each other, is performed, to establish a connection, c) *Security mode 3*, a device generates a PIN and transmits it securely to a second device, for display to the user, whereupon the user punches the same PIN onto a Bluetooth keypad for accomplishing mutual authentication, and d) *Security mode 4*, considered to be more secure than the other three approaches, uses a side-channel of communication (Near Field Communication) to exchange aspects of a secret (shared in this case), that is subsequently used by both devices for establishing a secure communication channel. All data communication post establishment of a connection is secured using public key cryptography.

Security mode 1 of Bluetooth does not provide protection against a man-in-the-middle attack, where an attacker can guise as user A and attempt to establish a connection by replaying a captured message (containing the encrypted PIN), directed from user A to user B, and thereupon hijacking all communication intended from user B to user A, without being traced. The ability of a security mode to ensure mutual authentication is therefore mandatory in ensuring the security of the Bluetooth communication protocol. The applications of Bluetooth in the context of the IoT infrastructure are in abundance primarily because of its convenient usage and minimal user intervention. For example, a travelling patient with a history of diabetes can have his or her blood sugar level tested using a Bluetooth-enabled mobile device, which can transmit the readings to a mobile reader at any healthcare checkup point at airports, train stations or even inside airplanes. Further communication of the readings from the device reader to a remote healthcare facility can be initiated upon a simple and automatic analysis of the readings by the device reader.

WI-FI SECURITY

While Bluetooth technology is intended for mobile devices and their interconnectivity, Wi-Fi is intended for establishing wireless local area networks on a larger scale, and provides users with on-the-fly connection to the Internet, through a device called the *hotspot*. Wi-Fi uses the Wi-Fi Protected Access (WPA and WPA2) standards to provide security to all communication channels. By default, Wi-Fi operates in an encryption-free mode (Lehembre, 2006). Therefore, unless an application service provider such as an online-banking server provides a secure communication channel (using HTTPS), it is not recommended to communicate passwords and other sensitive information through a Wi-Fi connection (as is also a rule of thumb for regular wired networks). Once enabled, WPA protects the Wi-Fi communication channel by generating a new key to protect each data packet transmitted from a device to the hotspot. The protocol generates keys based on passphrases entered by the user, for providing data encryption, message authentication code generation and verification, and mutual authentication. It may thus be noted that the security of the communication channel is very much dependant on the level of complexity of the passphrase chosen by a user. A simple passphrase may lead to a convenient compromise by an attacker, to launch attacks such as data capture, message replay, and data modification/erasure.

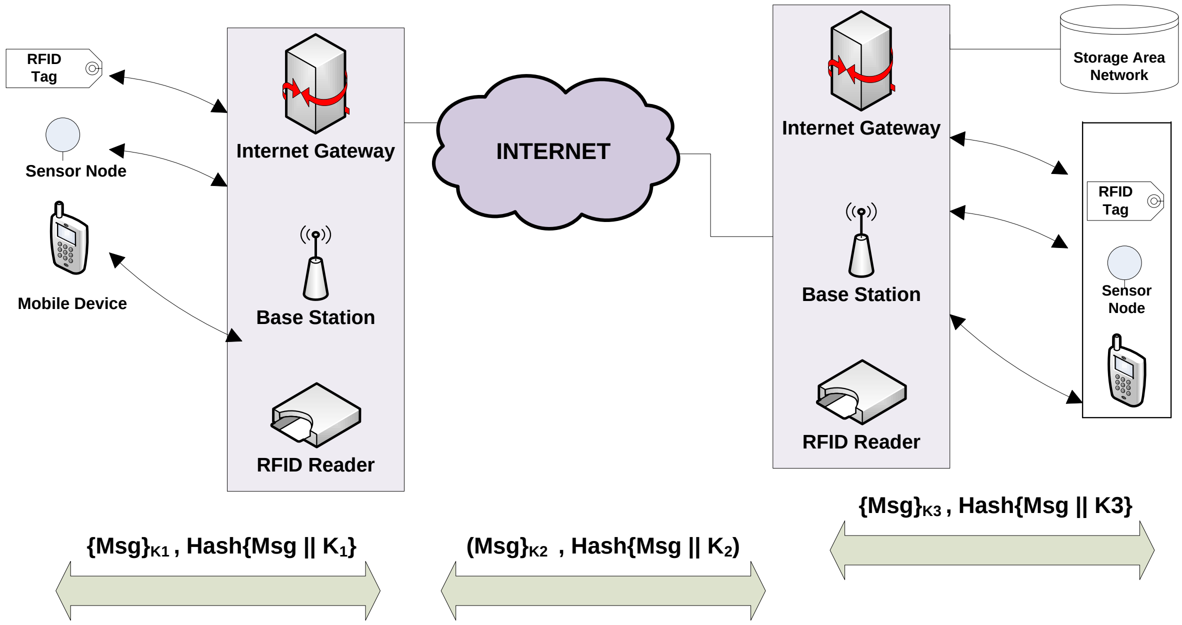
The Wi-Fi standard provides a very comfortable in-house network for a user to access the Internet. Wi-Fi hotspots are also available inside airplanes and at most airports and borders. A handicapped patient can remotely access the Internet from the comfort of his or her bed using a Wi-Fi connection. A device such as a sensor or an RFID tag connected to the patient's body, can transmit a reading securely to a Wi-Fi hotspot, for subsequent relay of the digitised record of the patient's readings to a remote healthcare facility. As a result, necessary support can be rendered if needed, or the patient may be advised on the dosage of medication to be taken, in a timely manner.

PARADIGMS FOR PROVISIONING SECURITY IN AN IOT INFRASTRUCTURE

A proposed paradigm for provisioning IoT security is to delegate all security-related operations to resource-rich Internet gateways and IoT device readers. The gateway in effect can follow standard public key or symmetric key cryptography for securing the communication channel between the source and the destination network. However, such an approach will not provide security for the IoT device-gateway communication channel. In Figure 2, a simple paradigm for providing a two-step approach for securing the IoT infrastructure is proposed. All devices with larger sets of information processing resources available to them are referred to as *facilitators* (includes gateways, RFID readers, base stations, etc). All communication between the IoT devices and the facilitators is secured using a shared key K_1. In particular, data is encrypted using the key K_{df}, and is transmitted alongside a message authentication code (MAC), where a MAC is the hash of the concatenation of the message to be transmitted, with a secret key shared between the sender and the receiver, using a standard hash function such as MD-5 or SHA-1. A message is thus appended with the MAC, and sent to the destination, where the MAC of the received message is recomputed and compared with the received MAC, for verification of message integrity and for authentication of the data source. Existing protocols such as Zigbee already have in-built data encryption procedures to secure the IoT device to intermediate facilitator communication channel.

A similar approach is followed to securely transmit data between the diverse facilitators through the Internet, albeit using a different key represented as K_2. The scheme used for data encryption and integrity check will depend on the capabilities of the device in question. For instance, a tiny RFID tag with limited processing capability will use symmetric encryption and smaller length keys, as opposed to a facilitator, which can use public key cryptography for ensuring communication channel security.

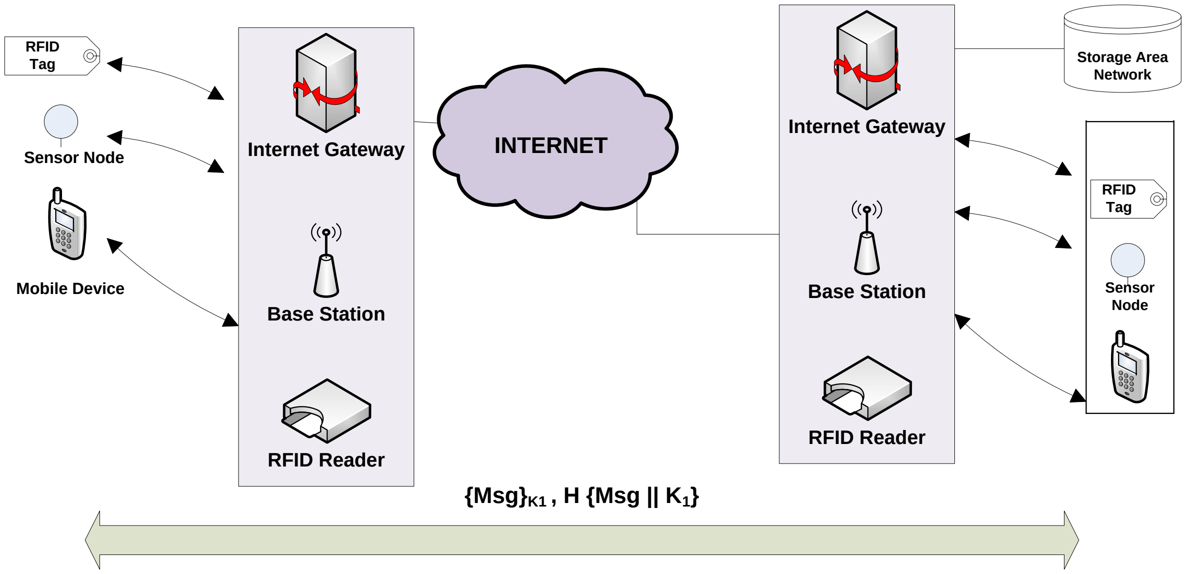
In Figure 3, an alternative paradigm towards securing the IoT is proposed, wherein all devices possess a distinct key to identify themselves in a global context, achievable only through the use of the IPv6 protocol. The IPv4 protocol is presently used for Internet communication. With growing number of Internet users, it is foreseen that unique IP addresses for devices connected to the Internet will eventually exhaust. As opposed to 32-bit addresses used by the IPv4 protocol, the IPv6 protocol, long overdue for deployment, will have 128-bits for addressing, to generate a total of 3.4 x 10^{38} distinct Internet addresses (Caicedo, 2009). With the growth of the IoT infrastructure gathering steam, it is anticipated that unique identification of devices across the world, based on their IP addresses will be realisable in the near future.



K_1 : Key shared between an IoT device and an intermediate facilitator.
K_2 : Key shared between two or more intermediary facilitators.
K_3 : Key shared between the destination IoT device and the facilitator.

Fig.2: A device-to-intermediary-to-device security paradigm for the IoT infrastructure.

Technological gaps or vulnerabilities in the contemporary IPv4 Internet architecture will also be experienced by end-users of the IoT infrastructure. It is therefore mandatory for having the resilience of such networks leveraged in time to accommodate these large set of electronic devices, which will inevitably dominate the market space in the near future. Such an infrastructure will place high demands on security, to be facilitated by the stakeholders (service providers). Therefore, the need for providing a coherent and effective end-to-end security mechanism applicable at the IoT infrastructure level, by mutual agreements and consortiums between the stakeholders of this vital infrastructure, cannot be understated.



K_1 : An end-to-end key shared between two or more IoT devices, uniquely possessed across the Internet.

Figure 3.An end-to-end secure channel for the IoT infrastructure (subject to availability of a unique key within each IoT device).

CONCLUSION

In this paper, a security assessment of technologies and standards of theIoT infrastructure were elaborated upon. As can be construed, the diversity in the range of devices that constitute an IoT, and the supported protocols, encumber the task of securing the end-to-end IoT communication channel. Two paradigms to secure an IoT infrastructure, namely, single key-based and two-step based, were proposed. The success of the IoTdepends on the close-knit coordination between all stakeholders for agreeing upon a standard approach towards securing the entire IoT infrastructure. A large set of diverse and independent security standards will encumber the process of securing the IoT infrastructure. It is therefore anticipatedthat a cumulative effort of all stakeholders of an IoT infrastructure will produce an effective ground for deployment of secure IoT-based services, to ascertain a convenient and safe end-user experience**.**

REFERENCES

Ari Juels, *RFID Security and Privacy: A Research Survey*, IEEE Journal on Selected Areas of Communications, vol. 24, no. 2, pp. 381-394, Feb. 2006.

Carlos E. Caicedo, James B.D. Joshi, Summit R. Tuladhar, *IPv6 Security Challenges*, Computer, vol. 42, no. 2, pp. 36-42, Feb. 2009.

Guillaume Lehembre, *Wi-Fi security - WEP, WPA and WPA2*,Haking- IT Security Magazine, vol. 14, no.1, Jan. 2006.

Hung-Min Sun, Shih-Pu Hsu, Chien-Ming Chen, *Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks*, in proc. of the Intl' Conf. on Advanced Information Networking and Applications Workshops, pp. 457-462, 2007.

Lu Yan, Yan Zhang, Laurence T. Yang, and Huansheng Ning. *The Internet of Things: Wireless Networks and Mobile Communications*, Taylor and Francis, 2008.

Masayuki Abe, M. McLoone, and M. Robshaw, *Public Key Cryptography and RFID Tags*, Lecture Notes in Computer Science, vol. 4377, pp. 372-384, 2006.

P. Bouska and M. Drahansky, *Communication Security in GSM Networks,*in proc. of the Intl' Conf. on Security Technology, pp. 248-251, 2008.

Sarah Rutlidge, *The PIC Farm: An Multiprocessor Sensor Board*,MSc Thesis, University of Lancaster, Sept. 2008.

Tzu-Chang Yeh, Yan-Jun Wang, Tsai-Chi Kuo, and Sheng-Shih Wang, *Securing RFID systems conforming to EPC Class 1 Generation 2 standard*, Expert Syst. Appl., vol. 37, no. 12, pp. 7678-7683, Dec. 2010.