Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 171-185 EISSN 2392-2192

Surveillance and Sequestration Issues of Internet of Things (SSIoT)

Reshma Banu[1], **Ayesha Taranum**[2]

Department of Information Science and Engineering, GSSS Institute of Engineering & Technology for Women, Mysore, India

[1,2]E-mail address: Reshma127banu@gmail.com , ayeshataranum@gsss.edu.in

ABSTRACT

A direct interpretation of the term Internet of Things refers to the use of standard Internet protocols for the human-to-thing or thing- to-thing communication in embedded networks. Although the security needs are well-recognized in this domain, it is still not fully understood how existing IP security protocols and architectures can be deployed. In this paper, we discuss the applicability and limitations of existing Inter- net protocols and security architectures in the context of the Internet of Things. First, we give an overview of the deployment model and general security needs. We then present challenges and requirements for IP-based security solutions and highlight technical limitations of standard IP security protocols. Focused on the security loopholes arising out of the information exchange technologies used in Internet of Things. No countermeasure to the security drawbacks has been analyzed in the paper.

Keywords**:** Denial of Service, RFID, WSN, Internet of Things, DDoS Attack, Surveillance, sequestration

1. INTRODUCTION

Building upon the concept of Device to Device (D2D) Communication technology of Bill Joy [1], Internet of Things (IoT) embodies the concept of free flow of information amongst the various embedded computing devices using the internet as the mode of intercommunication.

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

The term "Internet of Things" was first proposed by Kevin Ashton in the year 1982 [2]. With the aim of providing advanced mode of communication between the various systems and devices as well as facilitating the interaction of humans with the virtual environment, IoT finds its application in almost any field. But as with all things using the internet infrastructure for information exchange, IoT to is susceptible to various security issues and has some major privacy concerns for the end users. As such IoT, even with all its advanced capabilities in the information exchange area, is a flawed concept from the security viewpoint and proper steps has to be taken in the initial phase itself before going for further development of IoT for an effective and widely accepted adoption. In the Internet of Things (IoT), everything real becomes virtual, which means that each person and thing has a locatable, addressable, and readable counterpart on the Internet. These virtual entities can produce and consume services and collaborate toward a common goal.

The user's phone knows about his physical and mental state through a network of devices that surround his body, so it can act on his behalf. The embedded system in a swimming pool can share its state with other virtual entities. With these characteristics, the IoT promises to extend "anywhere, anyhow, anytime" computing to "anything, anyone, any service." Several significant obstacles remain to fulfill the IoT vision, among them security. The Internet and its users are already under continual attack, and a growing economy - replete with business models that undermine the Internet's ethical use - is fully focused on exploiting the current version's foundational weaknesses.

This does not bode well for the IoT, which incorporates many constrained devices. Indeed, realizing the IoT vision is likely to spark novel and ingenious malicious models. The challenge is to prevent the growth of such models or at least to mitigate and limit their impact. Meeting this challenge requires understanding the characteristics of things and the technologies that empower the IoT. Mobile applications are already intensifying users' interaction with the environment, and researchers have made considerable progress in developing sensory devices to provide myriad dimensions of information to enrich the user experience. The Thing Lifecycle and Architectural Considerations We consider the installation of a Building Automation Control (BAC) system to illustrate the lifecycle of a thing. A BAC system consists of a network of interconnected nodes that perform various functions in the domains of HVAC (Heating, Ventilating, and Air Conditioning), lighting, safety etc.

The nodes vary in functionality and a majority of them represent resource constrained devices such as sensors and luminaries. Some devices may also be battery operated or battery-less nodes, demanding for a focus on low energy consumption and on sleeping devices. In our example, the life of a thing starts when it is manufactured. Due to the different application areas (i.e., HVAC, lighting, safety) nodes are tailored to special task. It is therefore unlikely that a single manufacturer creates all nodes in a building. Hence, interoperability as well as trust bootstrapping between nodes of different vendors is important. The thing is later installed and commissioned within a network by an installer during the bootstrapping phase. Specially, the device identity and the secret keys used during normal operation are provided to the device during this phase. Different subcontractors may install different IoT devices for different purposes. Furthermore, the installation and bootstrapping procedures may not be a denned event but may stretch over an extended period of time. After being bootstrapped, the device and the system of things are in operational mode and run the functions of the BAC system. During this operational phase, the device is under the control of the system owner. For devices with lifetimes that span several years, occasional maintenance cycles may be required. During each maintenance phase, the software on the device can be upgraded or applications running on the device can be reconfigured. The maintenance tasks can thereby be performed either locally or from a backend system. Depending on the operational changes of the device, it may be required Security Challenges in the IP-based Internet of Things 3 to re-bootstrap at the end of a maintenance cycle.

The device continues to loop through the operational phase and the eventual maintenance phase until the device is decommissioned at the end of its lifecycle. However, the end-of-life of a device does not necessarily mean that it is defective but rather denotes a need to replace and upgrade the network to next-generation devices in order to provide additional functionality.

However, this separation of functionality adds further complexity and costs to the configuration and maintenance of the different networks within the same building. As a result, more recent building control networks employ IP- based standards allowing seamless control over the various nodes with a single management system. While allowing for easier integration, this shift towards IP-based standards results in new requirements regarding the implementation of IP security protocols on constrained devices and the bootstrapping of security keys for devices across multiple manufacturers.

2. CONNECTIVITY TECHNOLOGIES AND INTERACTION AMONGST VARIOUS INTERNET OF THINGS (IoT) DEVICES

The automatic exchange of information between two systems or two devices without any manual input is the main objective of the Internet of Things. This automated information exchange between two devices takes place through some specific communication technologies, which are described below.

2. 1. Wireless Sensor Networks (WSN)

As described in [3], A wireless sensor network (WSN) (sometimes called a wireless sensor and actuator network (WSAN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, [2] such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.

WSN are compositions of independent nodes whose wireless communication takes place over limited frequency and bandwidth. The communicating nodes of a typical wireless sensor network consist of the following parts:

i. Sensor
ii. Microcontroller
iii. Memory
iv. Radio Transceiver
v. Battery

Due to the limited communication range of each sensor node of a WSN, multi-hop relay of information take place between the source and the base station. The required data is collected by the wireless sensors through collaboration amongst the various nodes, which is then sent to the sink node for directed routing towards the base station. The communication network formed dynamically by the use of wireless radio transceivers facilitates data transmission between nodes. Multi-hop transmission of data demands different nodes to take diverse traffic loads.

Secure Interconnection between the IoT and Internet domains

The fundamental differences between the IoT domain and the Internet domain can be classified by the host and network capabilities as well as the respective network topology. Each dimension thereby shows challenges for standard IP security protocols to perform in the IoT domain:

1) Device capabilities: Internet hosts and IoT devices differ strongly regarding their available hardware resources. While Internet hosts are typically equipped with CPUs in the GHz range and several GBs of memory, embedded devices in the IoT domain are limited to CPUs in the MHz range and several KBs of memory. Recent IP security protocols cater for these differences of host capabilities by means of cryptographic agility concepts allowing for various ciphers for peer authentication. However, as the capabilities of a single Internet host compare to the capabilities of multiple IoT hosts, Internet hosts can mount attacks against IoT devices that are similarly effective to today's distributed Denial of Service attacks. DoS protection mechanisms built into standard IP security protocols do not mitigate this type of attack, as they often assume that individual hosts are equally powerful.

2) Network capabilities: The lossy communication channel, small packet sizes, and throughput in the order of tens of Kbit/sec for the IoT domain compare to a relatively reliable channel and high throughput the Internet. The lossy channel in the IoT scenario thereby demands for optimized protocol flows. Fate sharing of packet flights as implemented by (d)TLS is problematic, as the complete flights would need to be retransmitted in the likely event of packet loss. Additionally, different MTU sizes make fragmentation likely for packets originating from the Internet domain.6LowPAN compensates for this fact by handling packet fragmentation at its adaption layer. However, IP packet fragmentation enables malicious Internet hosts to fill up the limited buffer space of IoT hosts with invalid IP fragments by sending merely a few large packets. This is due to the fact that IP security protocols commonly calculate integrity checksums and signatures over whole packets instead of over intermediate fragments. Hence, the validity of fragmented packets cannot be verified before packet re-assembly.

3) Network topology: IoT networks denote wireless multi-hop routing structures, whereas the Internet backbone is wired and ISP-centered. The cooperative routing topology of IoT networks in combination with the higher bandwidth available to Internet host allows to not only target single IoT devices, but whole IoT networks with DoS attacks. As today's IP security protocols focus on end-to-end mechanisms, they do not defend against this type of attack that would need to stop at the IoT ingress point.The above issues show that IP security solutions do not cater immediately to a secure interconnection of IoT networks and the Internet. We now present an adaptation layer-based approach to enabling security bootstrapping between the IoT domain and the Internet with existing IP security protocols.

2. 2. Radio Frequency Identification (RFID)

In context to the Internet of Things (IoT), RFID is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader.

Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader and may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC) RFID technology is mainly used in information tags interacting with each other automatically. RFID tags use radio frequency waves for interacting and exchanging information between one another with no requirement for alignment in the same line of sight or physical contact. It uses the wireless technology of Automatic Identification and Data Capture (AIDC) .A RFID is made up of the following two components [2]:

2. 2. 1. RFID tags (Transponders)

In a RFID tag, an antenna is embedded in a microchip. The RFID tag also consists of memory units, which houses a unique identifier known as Electronic Product Code (EPC). The function of the EPC in each tag is to provide a universal numerical data by which a particular tag is recognized universally.

As per the classification in [2], the types of RFID tags are:

i. Active tag: This type of tag houses a battery internally, which facilitates the interaction of its unique EPC with its surrounding EPCs remotely from a limited distance.

ii. Passive tag: In this type of tag, the information relay of its EPC occurs only by its activation by a transceiver from a pre-defined range of the tag. The lack of an internal battery in the passive tags is substituted by its utilization of the electromagnetic signal emitted by a tag reader through inductive coupling as a source of energy. (For details about the utilization of external sources of energy in a passive tag, readers can refer to [4]).

A RFID tag operates in conjunction with a tag reader, the EPC of the former being the identifying signature of a particular tag under the scan of the latter.

2. 2. 2. RFID readers (Transceivers)

The RFID reader functions as the identification detector of each tag by its interaction with the EPC of the tag under its scan. More information on the working technologies behind RFID can be found in [6].

3. SECURITY ISSUES AND PRIVACY CONCERNS

Despite the immense potential of IoT in the various spheres, the whole communication infrastructure of the IoT is flawed from the security standpoint and is susceptible to loss of privacy for the end users.

Some of the most prominent security issues plaguing the entire developing IoT system arise out of the security issues present in the technologies used in IoT for information relay from one device to another. As such some of the prominent security issues stemming out from the communication technology are the following:

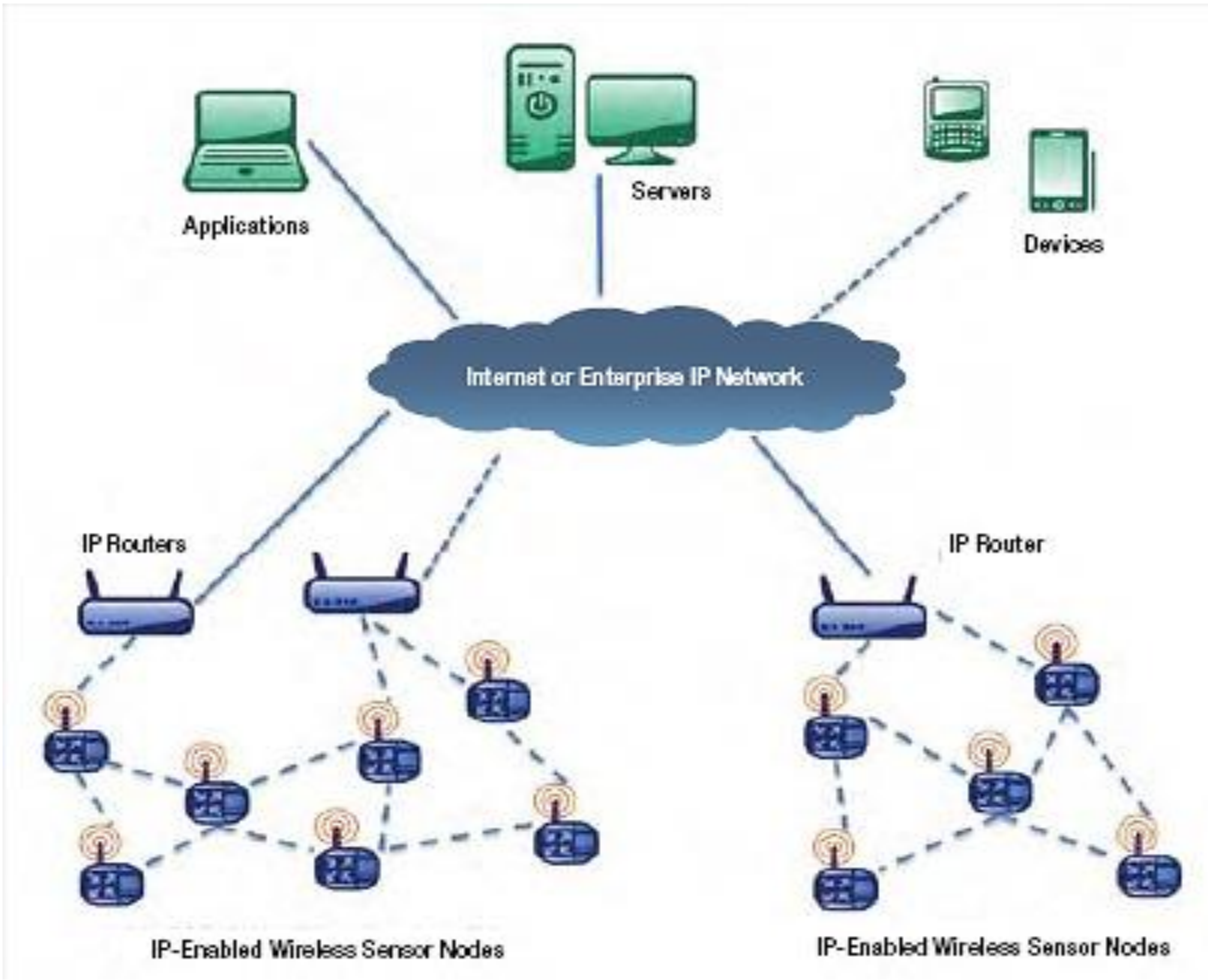
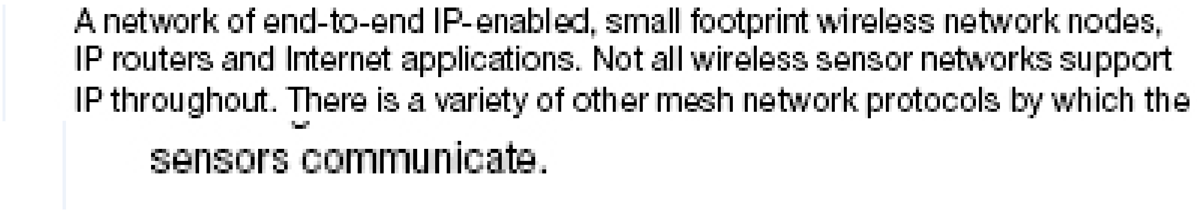
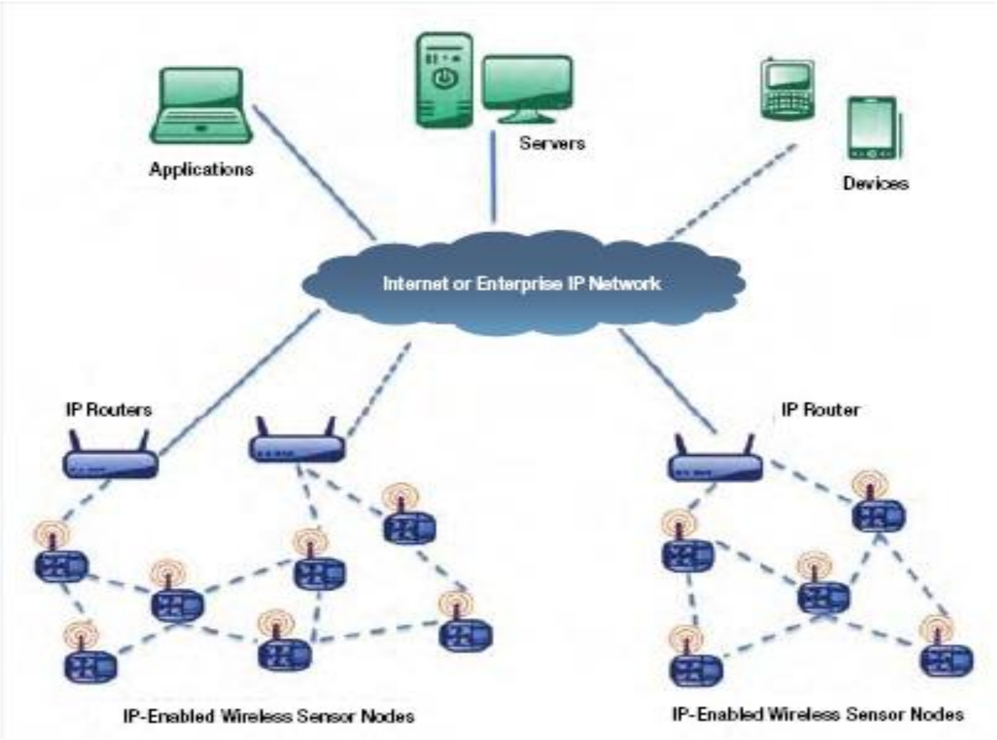

Applications
Servers
Devices
Internet or Enterprise IP Network
IP Routers
IP Router
IP-Enabled Wireless Sensor Nodes
IP-Enabled Wireless Sensor Nodes

Figure 1. Security in Wireless Sensor Networks


A network of end-to-end IP-enabled, small footprint wireless network nodes, IP routers and Internet applications. Not all wireless sensor networks support IP throughout. There is a variety of other mesh network protocols by which the sensors communicate.


Applications
Servers
Devices
Internet or Enterprise IP Network
IP Routers
IP Router
IP-Enabled Wireless Sensor Nodes
IP-Enabled Wireless Sensor Nodes

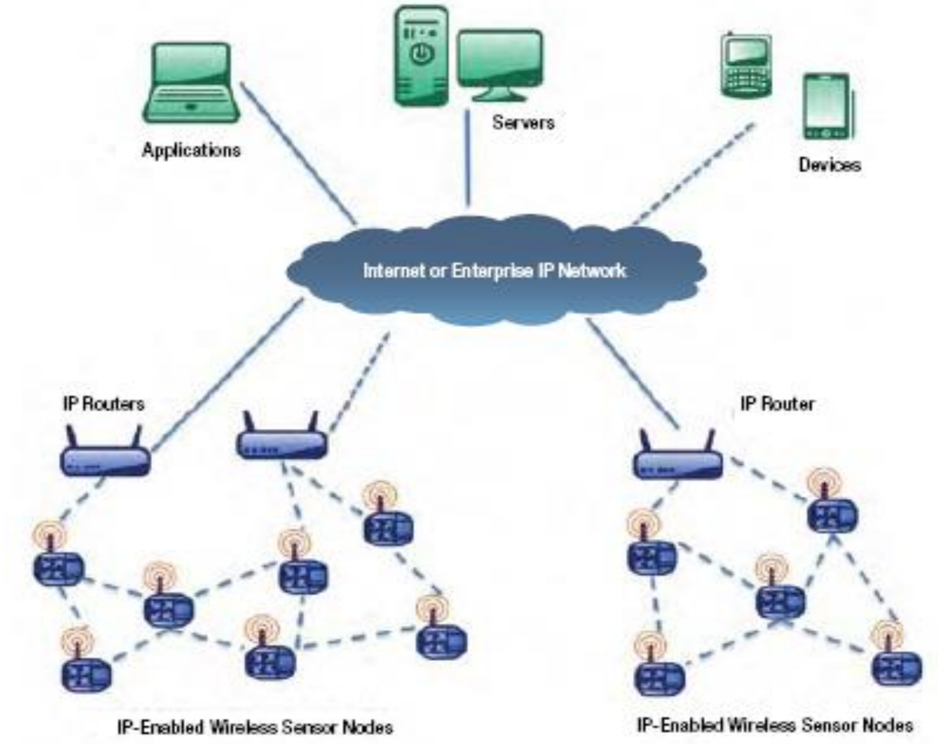
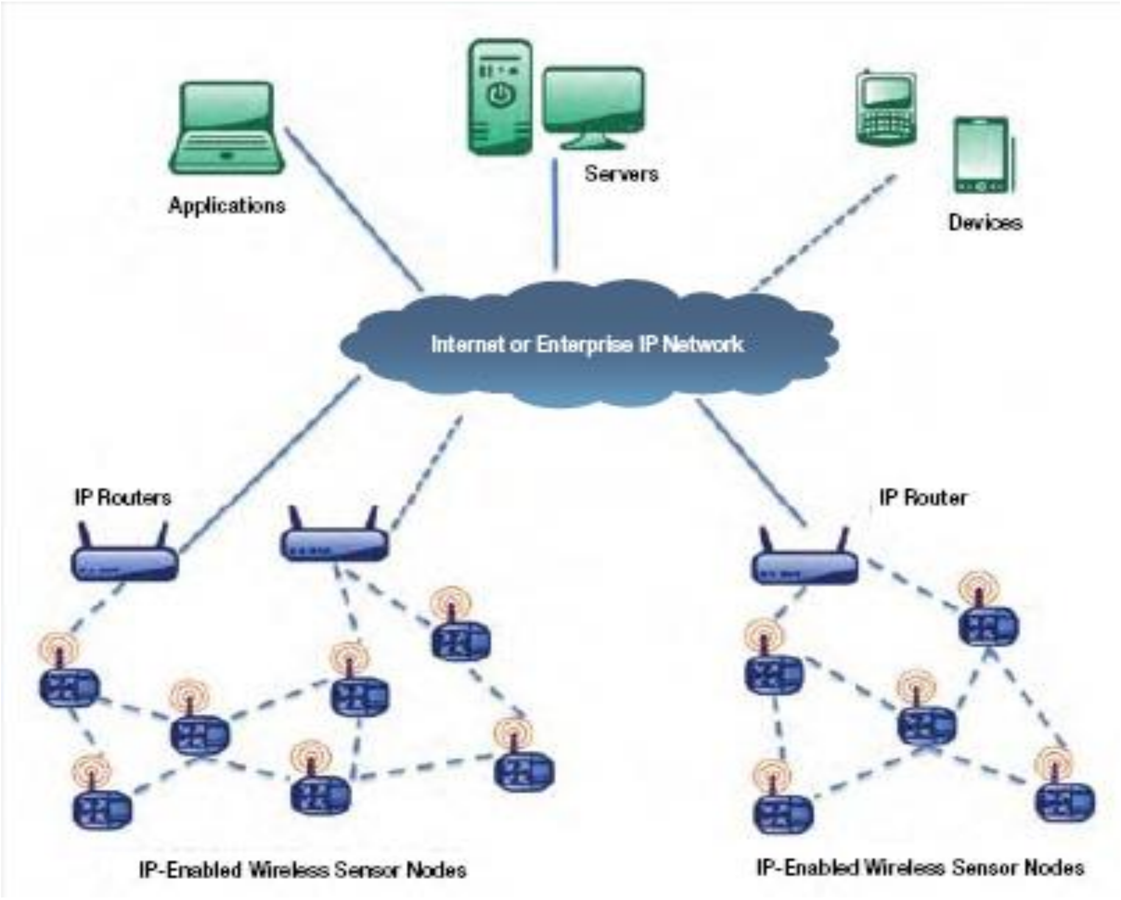

Applications
Servers
Devices
Internet or Enterprise IP Network
IP Routers
IP Router
IP-Enabled Wireless Sensor Nodes
IP-Enabled Wireless Sensor Nodes

FIGURE 2

A network of end-to-end IP-enabled, small footprint wireless network nodes, IP routers and Internet applications. Not all wireless sensor networks support IP throughout. There is a variety of other mesh network protocols by which the sensors communicate. Illustration courtesy Arch Rock.


Applications
Servers
Devices
Internet or Enterprise IP Network
IP Routers
IP Router
IP-Enabled Wireless Sensor Nodes
IP-Enabled Wireless Sensor Nodes

3. 1. Security issues in the wireless sensor networks (WSNs)

The hierarchical relationship of the various security issues plaguing the wireless sensor network is shown in Figure 2. The oppressive operations that can be performed in a wireless sensor network can be categorized under three categories [7]:

i. Attacks on secrecy and authentication
ii. Silent attacks on service integrity
iii. Attacks on network availability: The denial of service (DoS) ([16, 17]) attack falls under this category. This prevention of accessibility of information to legitimate users by unknown third party intruders can take place on different layers of a network [8, 14, 15].

3. 2. DoS attack on the physical layer

The physical layer of a wireless sensor network carries out the function of selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, transmission and reception of data [19]. This layer of the wireless sensor network is attacked mainly through

i. Jamming: In this type of DoS attack occupies the communication channel between the nodes thus preventing them from communicating with each other.

ii. Node tampering: Physical tampering of the node to extract sensitive information is known as node tampering.

3. 3. DoS attack on the link layer

The link layer of WSN multiplexes the various data streams provides detection of data frame, MAC and error control. Moreover the link layer ensures point-point or point-multipoint reliability [20]. The DoS attacks taking place in this layer are:

i. Collision: This type of DoS attack can be initiated when two nodes simultaneously transmit packets of data on the same frequency channel. The collision of data packets results in small changes in the packet results in identification of the packet as a mismatch at the receiving end. This leads to discard of the affected data packet for re-transmission [21].

ii. Unfairness: As described in [21], unfairness is a repeated collision based attack. It can also be referred to as exhaustion based attacks.

iii. Battery Exhaustion: This type of DoS attack causes unusually high traffic in a channel making its accessibility very limited to the nodes. Such a disruption in the channel is caused by a large number of requests (Request To Send) and transmissions over the channel.

3. 4. DoS attack on the network layer:

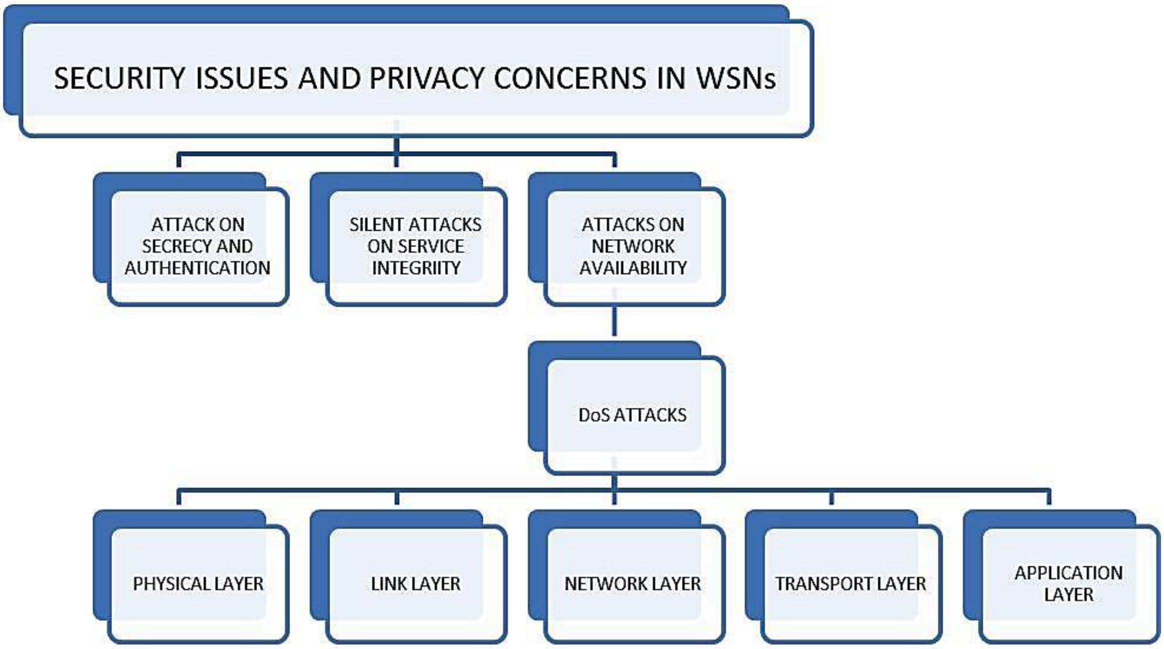

SECURITY ISSUES AND PRIVACY CONCERNS IN WSNs
ATTACK ON SECRECY AND AUTHENTICATION
SILENT ATTACKS ON SERVICE INTEGRIITY
ATTACKS ON NETWORK AVAILABILITY
DoS ATTACKS
PHYSICAL LAYER
LINK LAYER
NETWORK LAYER
TRANSPORT LAYER
APPLICATION LAYER

Figure 2. Hierarchical diagram of security issues in Wireless Sensor Network

The main function of the network layer of WSN is routing. The specific DoS attacks taking place in this layer are:

i. Spoofing, replaying and misdirection of traffic.
ii. Hello flood attack: This attack causes high traffic in channels by congesting the channel with an unusually high number of useless messages. Here a single malicious node sends a useless message which is then replayed by the attacker to create a high traffic.
iii. Homing: In case of homing attack, a search is made in the traffic for cluster heads and key managers which have the capability to shut down the entire network.
iv. Selective forwarding: As the name suggests, in selective forwarding, a compromised node only sends a selected few nodes instead of all the nodes. This selection of the nodes is done on the basis of the requirement of the attacker to achieve his malicious objective and thus such nodes does not forward packets of data.
v. Sybil: In a Sybil attack, the attacker replicates a single node and presents it with multiple identities to the other nodes.
vi. Wormhole: This DoS attack causes relocation of bits of data from its original position in the network. This relocation of data packet is carried out through tunnelling of bits of data over a link of low latency.

3. 5. DoS attack on the transport layer

This layer of the WSN architecture provides reliability of data transmission and avoids congestion resulting from high traffic in the routers. The DoS attacks in this layer are:

i. Flooding: It refers to deliberate congestion of communication channels through relay of unnecessary messages and high traffic.

ii. De-synchronization: In de-synchronization attack, fake messages are created at one or both endpoints requesting retransmissions for correction of non-existent error. This results in loss of energy in one or both the end-points in carrying out the spoofed instructions.

3. 6. DoS attack on the application layer

The application layer of WSN carries out the responsibility of traffic management. It also acts as the provider of software for different applications which carries out the translation of data into a comprehensible form or helps in collection of information by sending queries [20]. In this layer, a path-based DoS attack is initiated by stimulating the sensor nodes to create a huge traffic in the route towards the base station [21]. Figure 3 shows all the above mentioned DoS attacks in the different layers of a wireless sensor network.

Some additional DoS attacks are as follows [7, 14, 15]:

i. Neglect and Greed Attack
ii. Interrogation
iii. Black Holes
iv. Node Subversion
v. Node malfunction
vi. Node Outage
vii. Passive Information Gathering
viii. False Node
ix. Message Corruption

Some of the other security and privacy issues in a WSN are [7, 9, 10]:

i. Data Confidentiality
ii. Data Integrity
iii. Data Authentication
iv. Data Freshness
v. Availability
vi. Self-Organization
vii. Time Synchronization
viii. Secure Localization
ix. Flexibility
x. Robustness and Survivability

According to the threats looming over WSN can further be classified as follows:

i. External versus internal attacks
ii. Passive versus active attacks
iii. Mote-class versus laptop-class attacks

According to [12], the attacks on WSN can be classified as:

i. Interruption
ii. Interception
iii. Modification
iv. Fabrication

The attacks on WSN can further be classified as:

i. Host-based attacks
ii. Network-based attacks

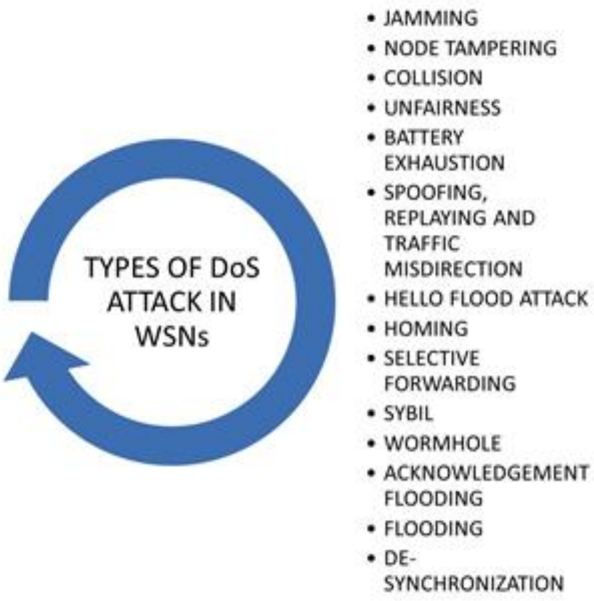


Figure 3. Types of Denial of Attack in Wireless Sensor Network

3. 7. Security issues in RFID technology

In context to IoT, RFID technology is mainly used as RFID tags for automated exchange of information without any manual involvement. But the RFID tags are prone to various attacks from outside due to the flawed security status of the RFID technology.

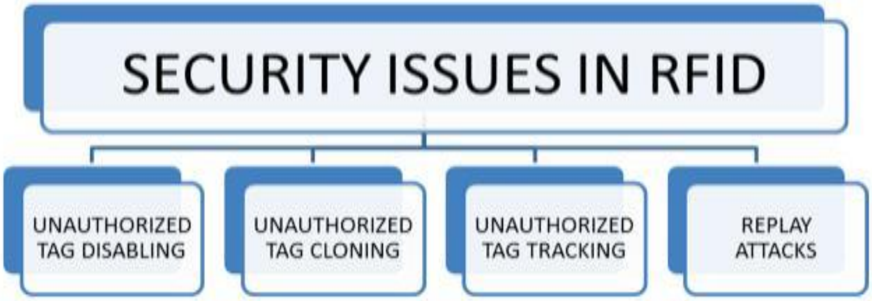


Figure 4. Security Issues in RFID

The four most common types of attacks and security issues of RFID tags are shown in Figure 4 which are as follows:

i. Unauthorized tag disabling (Attack on authenticity): The DoS attacks in the RFID technology leads to incapacitation of the RFID tags temporarily or permanently. Such attacks render a RFID tag to malfunction and misbehave under the scan of a tag reader, its EPC giving misinformation against the unique numerical combination identity assigned to it. These DoS attacks can be done remotely, allowing the attacker to manipulate the tag behavior from a distance.

ii. Unauthorized tag cloning (Attack on integrity): The capturing of the identification information (like its EPC) esp. through the manipulation of the tags by rogue readers falls under this category. Once the identification information of a tag is compromised, replication of the tag (cloning) is made possible which can be used to bypass counterfeit security measures as well as introducing new vulnerabilities in any industry using RFID tags automatic verification steps.

iii. Unauthorized tag tracking (Attack on confidentiality): A tag can be traced through rogue readers, which may result in giving up of sensitive information like a person’s address. Thus from a consumer’s viewpoint, buying a product having an RFID tag guarantees them no confidentiality regarding the purchase of their chase and in fact endangers their privacy.

iv. Replay attacks (Attack on availability): In this type of impersonation attacks the attacker uses a tag’s response to a rogue reader’s challenge to impersonate the tag In replay attacks, the communicating signal between the reader and the tag is intercepted, recorded and replayed upon the receipt of any query from the reader at a later time, thus faking the availability of the tag.

Besides this category, some prominent security vulnerabilities of RFID technologies are:

i. Reverse Engineering
ii. Power Analysis
iii. Eavesdropping
iv. Man-in-the-middle attack
v. Denial of Service (DoS)
vi. Spoofing
vii. Viruses
viii. Tracking
ix. Killing Tag Approach

3. 8. Security issues in health-related technologies built upon the concept of IoT:

Advances and convergence of engineering with biology has paved the way for wearable health monitoring devices which can constantly stream and share the information from the sensor of the health monitor with other devices and social network over the internet (The implementation of social connectivity with the sensor data can be found). The implementation of automatic collection of data by the sensors and uploading it to the various social networks through a web server introduces some high vulnerability in the whole data transmission process from the monitor to the Internet. On the basis of its target device (FITBIT), it has been recognized the following as the main security vulnerability in such health monitoring devices working in synchronization with the Internet:

Clear text HTTP data processing: The sensor data is sent to the web servers as plain HTTP instructions with no additional security or encryption. Such unprotected HTTP instructions can be easily intercepted for gaining access to various functions of a user account linked to the health-monitoring device.

From the above mentioned vulnerabilities it is clear that the security measures implemented in the health-related technologies which are socially connected over the internet lack the proper measures to address all the privacy concerns of the end users and puts the users at risk of exposing valuable information about their health to unknown personnel with malicious intents.

Based on the above-mentioned security flaws, many other security and privacy issues present themselves in the field of Internet of Things.

A few of them are:

- Theft of sensitive information like bank password
- Easy accessibility to personal details likes contact address, contact number etc.
- It may lead to open access to confidential information like financial status of an institution
- An attack on any one device may compromise the integrity of all the other connected devices. Thus the interconnectivity has a huge drawback as a single security failure can disrupt an entire network of devices.
- The reliance on the Internet makes the entire IoT architecture susceptible to virus attack, worm attack and most of the other security drawbacks that comes with any Internet connected computing device etc.

4. CONCLUSION

In this paper we have surveyed all the security flaws existing in the Internet of Things that may prove to be very detrimental in the development and implementation of IoT in the different fields. So adoption of sound security measures ([18]) countering the above detailed security flaw as well as implementation of various intrusion detection systems ([11]), cryptographic and stenographic security measures ([5]) in the information exchange process and using of efficient methods for communication ([13]) will result in a more secure and robust IoT infrastructure. In conclusion, we would like to suggest that more effort on development of secured measures for the existing IoT infrastructure before going for further development of new implementation methods of IoT in daily life would prove to be a more fruitful and systematic method.

References

[1] Jason Pontin. ETC: Bill Joy's Six Webs. In: MIT Technology Review, 29 September 2005. Retrieved 17 November 2013.

[2] Shen, Guicheng, and Bingwu Liu. "The visions, technologies, applications and security issues of Internet of Things." E-Business and E-Government (ICEE), *2011 International Conference on*. IEEE, 2011.

[3] Akyildiz, I.F. Georgia Inst. of Technol., Atlanta, GA, US ; Weilian Su; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *Communications magazine, IEEE* 40.8 (2002) 102-114

[4] Z.G. Prodanoff, Optimal frame size analysis for framed slotted ALOHA based RFID networks, *Computer Communications* (2009), doi: 10. 1016/j.comcom.2009.11.007

[5] S. Dey, A. Abraham and S. Sanyal, An LSB Data Hiding Technique Using Prime Numbers, *Third International Symposium on Information Assurance and Security*, 2007, pp. 101-108, doi: 10.1109/IAS.2007.37

[6] Rolf Clauberg. *RFID and Sensor Networks: From Sensor/Actuator to Business Application, RFID Workshop*, University of St. Gallen, Switzerland, September 27, 2004.

[7] Aashima Singla, Ratika Sachdeva, Review on Security Issues and Attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 4, April 2013.

[8] Sen, Jaydip. Security and privacy challenges in cognitive wireless sensor networks. arXiv preprint arXiv: 1302.2253 (2013).

[9] G. Bianchi, “A comparative study of the various security approaches used in wireless sensor networks,” *International Journal of Advanced Science and Technology*, Vol. 17, (2010) April, pp. 31-44.

[10] T. A. Zia, A Security Framework for Wireless Sensor Networks, http://ses.library.usyd.edu.au/bitstream/ 2123/2258/4/02whole.pdf, (2008).

[11] Bhattasali, Tapalina, Rituparna Chaki, and Sugata Sanyal. Sleep Deprivation Attack Detection in Wireless Sensor Network. arXiv preprint arXiv: 1203.0231(2012).

[12] Xiangqian Chen, Kia Makki, Kang Yen, Niki Pissinou, Sensor network security: a survey. *IEEE Communications Surveys and Tutorials* 01/2009; 11:52-73. DOI: 10.1109/SURV.2009.090205

[13] Roy, Bibhash, Suman Banik, Parthi Dey, Sugata Sanyal and Nabendu Chaki, Ant colony based routing for mobile ad-hoc networks towards improved quality of services. *Journal of Emerging Trends in Computing and Information Sciences* 3.1 (2012) 10-14

[14] M. Saxena, Security in Wireless Sensor Networks-A Layer based classification, Technical Report, Center for Education and Research in Information Assurance & Security-CERIAS, Purdue University. pages. cs. wisc.edu/~msaxena/papers/2007-04-cerias.pdf, (2007).

[15] J. Sen, A Survey on Wireless Sensor network Security. *International Journal of Communications Network and Information Security*, 1(2) (2009) 59-82.

[16] M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, *A Survey on Wireless Sensor Networks Security*. SETIT, (2007).

[17] T. Wang and H. Schulzrinne, An IP traceback mechanism for reflective DoS attacks. *Canadian Conference on Electrical and Computer Engineering*, 2 (2004) 901-904.

[18] Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal: A New Protocol to Counter Online Dictionary Attacks. *Computers and Security*, Volume 25, Issue 2, pp. 114-120, Elsevier Science, March, 2006. This paper is now listed in the top 25 articles of the COMPUTER SCIENCE (Computer and Security)

[19] http://sensors-and-networks.blogspot.in/2011/08 /physical-layer-for-wireless-sensor.html

[20] Al-Sakib Khan Pathan, Denial of Service in Wireless Sensor Networks: Issues and Challenges. Advances in communications and Media Research, ISBN 978-1-60876-576-8