Classification Mechanism for IoT Devices towards Creating a Security Framework

V.J. Jincy and Sudharsan Sundararajan

Abstract. IoT systems and devices are being used for various applications ranging from households to large industries on a very large scale. Design of complex systems comprising of different IoT devices involves meeting of security requirements for the whole system. Creating a general security framework for such interconnected systems is a challenging task and currently we do not have standard mechanisms for securing such systems. The first step towards developing such a framework would be to build a classification mechanism which can identify the security capabilities or parameters of the different entities comprising an IoT system. In this paper we describe one such mechanism which can take user input to classify the different components of a complex system and thereby determine their capability to support security mechanisms of different degrees. This in turn would enable designers to decide what kind of security protocols they need to adopt to achieve end-to-end security for the whole system.

Keywords: Internet of Things, IoT devices, Properties, Security Properties, Classification, Security Parameters.

1 Introduction

Internet-of-Things (IoT) is the latest paradigm to capture the interest and imagination of not only the scientific and research community but also that of the common man. With the advent of high tech, smart gadgets and the enormous increase in communication bandwidth and availability, the number of novel applications to enhance the quality of life of the common man has increased exponentially within

V.J. Jincy · Sudharsan Sundararajan
Amrita Center for Cyber Security
Amrita Vishwa Vidyapeetham
Kollam, India
e-mail: jincyvalsan87@gmail.com,
sudharsan@am.amrita.edu

R. Buyya and S.M. Thampi (eds.), *Intelligent Distributed Computing*,
Advances in Intelligent Systems and Computing 321, DOI: 10.1007/978-3-319-11227-5_23

the last few years. Although the term Internet-of-Things was coined as early as in 1999 when radio-frequency ID (RFID) tags were used to identify and manage products and inventories, the technology has become more pervasive and taken center stage in the recent years. With intelligent systems, automation and remote operations being enabled by the revolution in communication and computing technologies, the importance of the idea of operating in an environment where things interact with human beings and also amongst themselves has become a reality. With such complex systems invading our day-to-day lives the security of information handled and our interactions with such devices takes paramount importance.

Many of our current intelligent systems are a combination of sensors, actuators and networked intelligence. The components comprising these systems can be anything from humans to machines which could be connected and interact amongst themselves. Due to the increasing use of variety of IoT devices in various fields these devices and systems need to have assured secure and safe operation. Currently we do not have specific security mechanisms or standards for different devices and their interoperability. When it comes to the case of large or small IoT systems comprising of various IoT devices the idea of defining a common security framework is yet to be done. The first steps to create a security framework for an IoT system would be to classify the various devices that comprise the system with respect to their capabilities in terms of computing, communication and other important parameters. We have not come across any such direct classification mechanism of this kind in this scenario which would help identify the capabilities of the devices rather than data they handle. In this work we present a different approach to classify the various IoT devices into three distinct classes namely Class A, Class B, Class C with security levels defined as High, Medium and Low respectively. This we take as our first step towards developing a generic security framework for systems that are built by different IoT devices that are interoperable. In Section 2 we describe the existing work that has been done in the field of classification and security of IoT systems. The next section describes about the system design wherein the different properties of the IoT devices which would help in the classification mechanism are listed and discussed. Section 4 describes the shortlisted properties and their usage in the classification mechanism. The section also describes the different IoT systems that were selected as test inputs to the classifier and their classification. We conclude the paper in section 5 stating the use of the classification in creating a security framework for IoT systems.

2 Related Work

Classification becomes important when the concern comes to assigning security levels to IoT systems currently in use and also those which are yet to come. An Ontology based classification [1] was done initially in this field which mainly

dealt with two issues that is Heterogeneous Device integration and Composite event detection. In [1] authors have also mentioned about four classes in the first tier which are Places, Nodes, Sensors and Events. The classification was done on wireless sensor networks based on ontology as the name suggests. Next is about the device centric approach for a safer IoT where four different categories were considered by the authors in [2] where devices are supposed to be under risk and these were Hostile Environment, Interference, Misuse, and Internal Failures. The safety concepts were defined staying outside the domains of applications. Context was also a matter of concern there. Context based entities were defined for the first time in [2].The thought of considering the context for the classification came from [2] which was completely novel in the realm of IoT. While considering the security aspect of these devices mainly two types of security [3] was considered namely communication and physical level of security where the communication level [4] was given more importance as the different IoT devices were considered working together in co-ordination. In [4] authors have mentioned about the various issues occurring during the communication of different devices comprising of wireless sensors and actuators which is considered as a reference for analyzing the level of communication security required in each of the listed devices. More description about the security based classification is discussed in the last section. In [5], [6] and [7] the authors have provided a detailed account on the various properties of the IoT devices. They have also discussed about the different scenarios where these are used. In [8] they have discussed in detail about the health status monitoring node from which we could get a detail account about such devices used in the health care. The main concept behind the working of the sensor node is discussed in [9] which have helped a lot in our research work. The network based fire detection system was discussed in [10] which provided us with important information for selecting many of the devices and nodes. In [11] authors have discussed about the devices used for monitoring the environmental parameters. From [12] and [13] we could find some of the devices utilizing the advanced technologies used in industries and make use of their properties for our research. In [15] the authors have done analytical experiments on the working of air traffic control node using formal methods which shows the requirement of a high level of security in the system. Finally in [16] and [17] weka tool (developed by Waikato University in New Zealand) is being discussed which is mainly used for classification, regression, clustering, and association purposes. This tool has been used for the classification in this paper.

3 System Design

Here we describe how we are identifying the various properties of the IoT devices and systems and also discuss about building a classification tree based on the identified properties. This will serve as initial inputs to generate data for the IoT device classification.

3.1 Properties

As a first step we listed out a number of IoT devices and systems and identified their properties which can take on different types of values. Some of the identified properties are discussed below.

Power Constrained or Non Power Constrained. Power constrained systems are mostly working with battery backup and once the battery power is off the system stops working. For example a sensor which is to sense a value every 20 seconds, it senses for 5 seconds and goes off to sleep for 15 seconds thereby conserving power but if this system is compromised then power could be drained by not allowing it to go to sleep. When the power ceases working of the device stops which is a security issue. Non power constrained systems will have a continuous power back up. Values are two

Real Time or Non Real Time. Real Time systems must process information and produce a response within a specified time otherwise results in severe consequences for example Medical devices, Aircraft control and Nuclear Plant management. Non Real time systems process information and produce response but there is no specific time or deadline for that for e.g.: Behaviour Analysis Systems. Values are two.

Closed Loop and Open Loop. Closed loop systems are those which have a feedback mechanism for e.g.: Automated industrial control systems may be used for controlling the amount of water entering into the nuclear reactor at a particular temperature. Open loop systems are those used just for monitoring purposes like weather monitoring. Values are two.

Communication Protocol Used. Devices need to communicate with each other effectively and so different communication protocols are used for communication among these devices e.g.: TCP, UDP, PPP, IGMP, CLNP etc...

Wired and Wireless Systems. Here communication is wired or wireless. It is a physical layer Property. It directly relates to power constrained or non power constrained. Wired examples are RJ45, RS232, Twisted pair, Coaxial cable, Optical fibre Communication. Wireless examples are: Wi-Fi IEEE 802.11, Bluetooth, Infra red, GSM, WiMax IEEE 802.16

Network Size. Based on different application domains size of the network can be the following: Small Medium and large. The application domains can be Smart home/office where the area is very small and number of users is also limited so a small network will do. In case of Smart transportation it includes vast geographical area hence we need a large network size. In case of Smart city we can have a medium network size. Values are: Small, Medium, and Large.

Interoperability. A device can be considered as interoperable if it is compatible in two different networks like for example a device compatible with Bluetooth as well as WiFi.

Reliability. A system is said to be reliable if it has a back up mechanism. (Backing up means copying or archiving data so that the data could be restored once it is lost due to some error or crash) For example in case of sensors deployed in hostile environments if in any case it crashes if it has a backup mechanism then the data sensed so far could be recovered. Hence we can say that the system is reliable but this is not possible then it is an unreliable system

Energy Source. System utilizes energy in different means like it can be Rechargeable battery or Energy harvesting (also known as power harvesting where energy is derived from external sources like solar power, thermal Energy, wind energy, is captured and stored for small, wireless autonomous devices.)So based on the application domain it can be either of them or may be both. In case of Smart home/office it is rechargeable battery, in case of smart city we have both rechargeable battery and energy harvesting.

Processing Speed. It is the measure of cognitive efficiency. The ability to perform a task automatically and speedily in a system. The processing speed of each and every sensor network varies. It can take only a definite value.

Data Management. Data management in case of various systems is basically through Local server or shared server both. In case of smart homes/office a local server does the data management. In case of Smart Transportation shared server does. In Smart Agriculture both local server and shared server does data management. Values are 2: Shared server/Local server

Memory. The storage space required is defined as memory in terms of megabytes, gigabytes etc.... So it can take only a single value. Based on the range of values we can divide it into 3 categories namely low, medium and high for less than 10KB, between 10KB & 1GB and above 1 GB respectively.

Scalability. Depends on the utility of various sensors whether they are used on a large scale, small scale or medium scale. Large scale means usage in an industry in large number, small scale means a limited number of sensors used for a particular purpose may be in a house. Medium scale refers to number of sensors used in places like banks or airports etc…

Bandwidth. The band-width requirement for different systems or devices is different based on their functions. It can take three values .i.e. Low, Medium or High

Size of Sensors. The size of the sensors used in various devices also changes based on the requirements of the device and the application to be performed

Functionality. Functionality means whether it is a critical or noncritical one.

3.2 Classification Tree

Different properties have already been listed in the previous section and based on those properties we built a classification tree in order to identify the important properties among those to be finalized for classification. When the classification tree is built the main node which is the root of the tree is taken to be the important one among the remaining ones (nodes) since the remaining ones can be derived easily from the root. The main node is IoT devices which are further divided into 7 categories and split into sub categories. These categories are size, Type of node, Network layer, System, Scalability, Power and Processing.

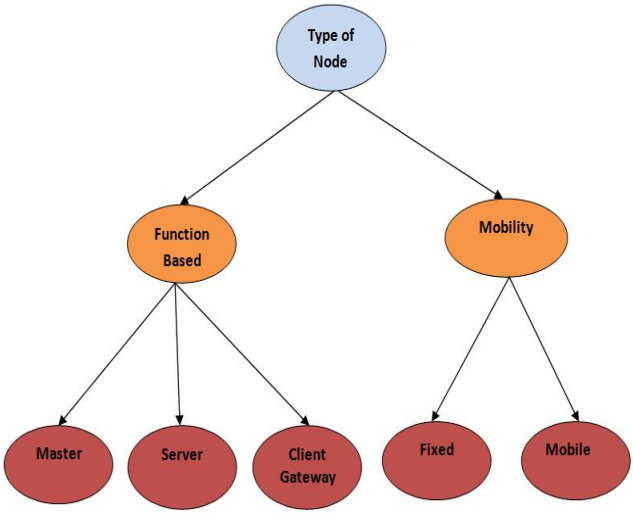

Fig. 1 Classification based on Node Type

Type of node is divided into two namely function based and mobility of the node. This specially relates to the usage scenario of the devices and also the specific nodes acting as master, server and client gateway. The mobility refers to whether the node is movable or not (Fixed or Mobile).

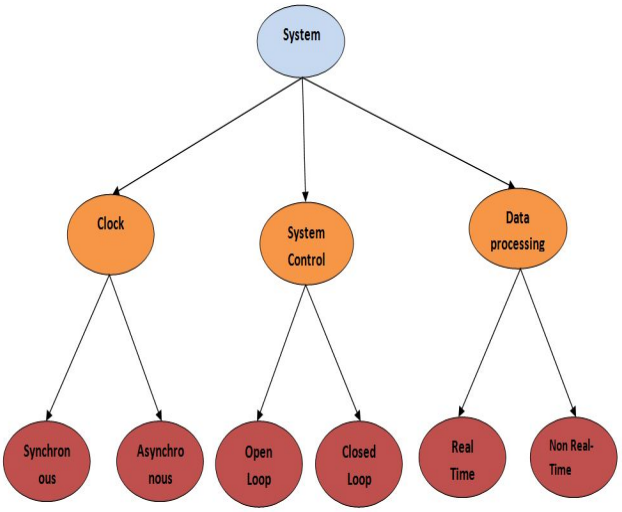

Fig. 2 Classification based on System Parameters

The remaining part is discussed in the next section which is implementation where we have the major task leading to the classification mechanism.

4 Implementation

After the identification of the various properties discussed in the above section the important aspect of the classification is to identify the properties that are important from the standpoint of building a secure system. Hence we have chosen some of the properties from those used to build the classification tree. Also we have chosen a few devices and systems for classification and have discussed their properties and classification

4.1 Finalized Properties

The list of identified properties is as follows

- Connectivity (Wired/Wireless)
- Real-Time (Yes/No)
- Power (Constrained/Non Constrained)
- Device Type (Sensor, actuator, hybrid)
- System Control (Open loop, closed loop)
- Functionality (Critical, Non Critical)

4.2 Device Classification

Here we list out the IoT devices and some applications based on them and the classification of the devices based on their properties. Around 20 devices were selected based on different references and also randomly from internet. These are the list of devices and their brief description along with their properties.

Fire Detection and Extinguishing System

1. Fire Detection Sensor Node
   Wireless, Real time, Non Power Constrained, Sensor, Open Loop, Critical

2. Sprinkler Node
   Wireless, Real-Time, Non Power constrained, Actuator, Open loop, Critical

Industrial Systems

3. Laser Distance Meters: Measure distances and speed in a non contact fashion and also without reflectors
   Wireless, Real Time, Power Constrained, Sensor, Closed loop, Non Critical

4. Thermography Camera module: For accurately measuring or visualizing heat distributions , outputs radiometric images of up to 2048 x 1536 pixel spatial resolution in real time.
   Wireless, Real Time, Power Constrained, Sensor, Closed loop, Non Critical

Home Automation

5. Smart Meters: A **smart meter** is an electrical meter which performs the function of recording the amount of electric energy consumed in intervals of an hour or less and passes on the data to the main utility for monitoring and billing purposes thereby which a two-way communication is established between the meter and the main system and could gather data for remote reporting.
   Wired, Non Real Time, Non Power Constrained, Sensors, Closed loop, Non Critical

6. Motion Detection Sensors in home: A **motion detector** is a device that detects moving objects, particularly people (as they are always in motion). A motion detector is often integrated as a component of a system that automatically performs a task or alerts a user of motion in an area. Motion detectors form a vital component of security, automated lighting control, home control, energy efficiency, and other useful systems.
   Wireless, Real time, Power constrained, Sensor, Open loop, Non critical

7. Smart Bulbs: WiFi enabled, energy efficient LED light bulb that can be controlled using your Smartphone.
   Wired, Non Real Time, Non Power Constrained, Sensors, Closed Loop, Non Critical

Health Care

8. Pacemaker: A pacemaker is a small device placed in the chest or abdomen which helps in controlling abnormal heart rhythms. This device uses electrical pulses to prompt the heart to beat at a normal rate. A pacemaker consists of a battery, then a computerized generator, and also wires with sensors at their tips called electrodes. The generator is powered by the battery, and both of these are surrounded by a thin metal box. The wires connect this generator to the heart.
Wireless, Real Time, Power Constrained, Sensors, Closed loop, Critical

9. Health Status monitoring node: The integration of various technologies RFID, GPS, GSM and GIS to construct a stray prevention system for the elderly that does not interfere with the elders' daily lives**.** RFID is the monitoring node.
Wireless, Real Time, Power Constrained, Sensors (RFID Sensors), Open loop, Critical

Monitoring Nodes

10. Air traffic Control node: It is found that airspace system's capacity and safety are largely dependent on the efficient coordination of air traffic control (ATC) and flight desk personnel. Smart Air Traffic control systems are designed consisting of a Controller, Aircraft, and Network state Controller.
Wireless, Real Time, Power constrained, Actuator, Closed loop, Critical.

11. Weather monitoring node: Modern weather forecast are result of a computer calculated model which uses weather stations and satellites around the world. It consists of sensors, Timers, multiplexer etc…
Wireless, Real Time, Power Constrained, Sensor, Closed Loop, Non Critical.

12. Earthquake Detection node: A seismic monitoring and Alarm System have been developed for intelligent structures. It consists of sensor nodes for sensing the earthquake tremors.
Wireless, Real Time, Power Constrained, Sensor, Closed loop, Critical

13. RFID Smart Conveyor Belt with Confined Detection Range: Radio Frequency Identification (RFID) technology enables detection and recognition of objects associated to univocal identification codes. A typical RFID system comprises an RFID reader linked to one or several antennas that interrogate the tags within its detection range.
Wired, Real Time, Non power constrained, Sensors (RFID smart conveyor belt), closed loop, Non Critical

14. Land Traffic Control node: Smart Traffic control systems are designed using wireless sensor network which also detects over speeding vehicles.
Wireless, Real Time, Power Constrained, Sensors, Closed loop, Critical

15. Smart cars sensor node: Modern day cars are equipped with LCD screens, GPS navigation, Sensors telephone and radio controls etc…
Wired, Real Time, Power Constrained, Sensors, Open loop, Critical

16. Irrigation Systems sensor nodes: Distributed in-field sensor-based irrigation systems offer a potential solution to support site-specific irrigation management that allows producers to maximize their productivity while saving water. Consists of wireless sensor network, software for real time in field sensing.
Wireless, Real Time, Power Constrained, Sensors, Open Loop, Non Critical

17. Amrita Personal Safety system: Wearable and easy to operate electronic device which helps to trigger communication with family and police when in distress.
Wireless, Real Time, Power constrained, Actuator, Open Loop, Critical

18. Traffic surveillance camera module: Cameras used for Traffic surveillance especially to point out whether there is any traffic rules violation. CMOS sensors are used.
Wireless, Real time, Power constrained, Sensor, Closed loop, Non critical.

19. Deep ocean tsunami detection buoys: Deep-ocean tsunami detection buoys are one among the two types of instruments being used by the Bureau of Meteorology (Bureau) to confirm the occurrence of tsunami waves generated by earthquakes undersea. These buoys are meant for observing and recording changes in sea level out in the deep ocean.
Wireless, Real time, Power constrained, Sensor, Closed Loop, Critical

4.3 Classification Algorithms

There are several classification algorithms which can be used for classifying the different devices we have. Since there were no existing databases for the IoT devices we just created our own database with all devices and their respective properties listed out. Naive Bayes algorithm was found to be appropriate for the classification purpose. Weka tool was used to carry out the whole process of classification where the csv (Comma separated Value) file is provided as input. This file consists of listed properties separated by commas. We get a complete analysis graph and also the confusion matrix from the weka tool from which we can easily make out the different classes as Class A, Class B and Class C. Class A for Critical, Class B for Medium and Class C for Non critical. After the initial classification we switched on to the context based approach in which we included the context in which each device is used as a new property among the existing list of properties. The same procedure was followed as done in previous case mentioned above. Finally we were able to classify the devices to Class A, Class B, and Class C for Critical, Medium and Non critical respectively. We could get the same result as before.

To enhance our findings we considered the security properties as well along with the previous classification and finally obtained a classified set consisting of 3 classes namely Class A, Class B, Class C for High level of security, medium and low level of security respectively. From the obtained result we could infer that our results are correct and if we need to know the security requirement of any IoT device there is just a need to list out properties in csv file and provide as test input. After receiving this test input the weka tool using the Naïve Bayes algorithm compares with the above obtained result and assigns a class for the test input comprising of properties. The output would be displayed in the weka console as one of the three .i.e. Class A, Class B, Class C.As an enhancement to this we can consider the whole system with a wide variety of IoT devices coming under different classes. When the user is able to provide information to a system or tool about the properties of the IoT system to be constructed then using the provided information we can create a csv file which would now be used as a test input and finally the Class of the system could be predicted. This is how we can arrive at the development of a security framework using the existing classification mechanism mentioned in this paper. This security framework would be beneficial in every aspect for the IoT systems yet to be developed.

4.4 Security Framework Creation

The proposed security framework is developed by first grouping the properties of different security protocols like ZigBee, Bluetooth, 6Lowpan, Ethernet and NFC along with the existing security mechanisms in them. The different properties considered were power requirements, Processing power, Net bandwidth, Application, Working Range and network topology. The findings are tabulated and results are obtained after proper analysis of the existing security mechanisms such as the cryptographic techniques and error detection mechanisms being used in those protocols. Based on these properties we carried out the classification as done in the previous section and obtained Class A security suit, Class B suit and Class C suit respectively for Class A, Class B and Class C devices used in creating a new smart system. The created user interface allows the user to enter the details of the devices to be used in creation of new system. Once the details are entered we have a csv file generated with all the properties listed. Once this file is obtained we can manually decide as to which protocol suits it the best based on the previous results and the tabulated data highlighting the security mechanisms used in various protocols mentioned in the beginning. So finally we arrive at a single or may be pairs of protocols compatible with the current system being designed which would provide it the maximum, medium or minimum security based on the context where the system is used. This would be used as the generalized method of assigning security levels to the complex sophisticated smart systems to be designed in the future.

5 Conclusion

The classification mechanism for the IoT devices presented above will help to identify the different security capabilities of the devices by assigning them a particular class and at the same time help the system designers to evolve a security mechanism for the whole system taking into consideration the different classes of devices that need to interact in the system. This will help to act as a foundation for building a generic security framework guideline wherein a system designer can choose from a range of security protocols available for different classes of devices which he can integrate to achieve the required security level for the whole system.

References

1. Danieletto, M., Bui, N., Zorzi, M.: An Ontology-based Framework for Autonomic Classification. In: 2011 IEEE International Conference on Internet of Things Communications Workshops (ICC), pp. 5–9 (2011)
2. Chen, C., Helal, S.: A Device-Centric Approach to a Safer Internet of Things. In: NoME-IoT 2011 Proceedings of the 2011 International Workshop on Networking and Object Memories for the Internet of Things. ACM, New York (2011)
3. Weingart, S.H.: Physical Security Devices for Computer Sub systems: A Survey of Attacks and Defenses. In: CHES 2008 Version (2008)
4. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., Srivastava, M.B.: On Communication Security in Wireless Ad-Hoc Networks. In: Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002) (2002)
5. Yang, D.-L., Liu, F., Liang, Y.-D.: A Survey of the Internet of Things. In: The International Conference on E-Business Intelligence (2010)
6. Gubbia, J., Buyyab, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): A vision, architectural elements, and future directions
7. Agrawal, S., Vieira, D.: A survey on Internet of Things
8. Barger, T.S., Brown, D.E., Alwan, M.: IEEE Health-Status Monitoring Through Analysis of Behavioral Patterns. IEEE Transactions On Systems, Man, And Cybernetics (January 2005)
9. Chong, C.-Y., Kumar, S.P.: Sensor Networks: Evolution, Opportunities,and Challenges. Proceedings of the IEEE (August 2003)
10. Lee, K.C., Lee, H.-H.: Network-based Fire-Detection System via Controller Area Network for Smart Home Automation. IEEE Transactions on Consumer Electronics (November 2004)
11. Haefke, M., Mukhopadhyay, S.C., Ewald, H.: A Zigbee Based Smart Sensing Platform for Monitoring Environmental Parameters. In: 2011 IEEE Instrumentation and Measurement Technology Conference, I2MTC (2011)
12. Official website of Jenoptik `http://jenoptik.com` (accessed on November 2013)
13. Official Website of Beecham Research, `http://beechamresearch.com/article.aspx?title=Research` (acesses on November 2013)

14. Wikipedia on Internet_of_Things: wikipedia.org/wiki/Internet of Things
15. Jamal, M., Zafar, N.A.: Requirements Analysis of Air Traffic Control System Using Formal Methods
16. Official Website of waikato university, http://cs.waikato.ac.nz/ml/ (accessed on November 2013)
17. Frank, E., Trigg, L., Hall, M., Holmes, G., Kirkby, R., Pfahringer, B., Witten, I.H.: Weka: A Machine learning Workbench for data mining