Object Classification based Context Management for Identity Management in Internet of Things
Mahalle, Parikshit N.; Prasad, Neeli R.; Prasad, Ramjee

Published in:
International Journal of Computer Applications

DOI (link to publication from Publisher):
10.5120/10515-5486

Publication date:
2013

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Object Classification based Context Management for Identity Management in Internet of Things

Parikshit N. Mahalle  
Center for TeleIn Frastruktur, Aalborg University, Aalborg, Denmark

Neeli Rashmi Prasad  
Center for TeleIn Frastruktur, Aalborg University, Aalborg, Denmark

Ramjee Prasad  
Center for TeleIn Frastruktur, Aalborg University, Aalborg, Denmark

ABSTRACT
As computing technology is becoming more tightly coupled into dynamic and mobile world of the Internet of Things (IoT), security mechanism is more stringent, flexible and less intrusive. Scalability issue in IoT makes identity management (IdM) of ubiquitous objects more challenging, and there is a need of context-aware access control solution for IdM. Confronting uncertainty of different types of objects in IoT is not easy. This paper presents the logical framework for object classification in context aware IoT, as richer contextual information creates an impact on the access control. This paper proposes decision theory based object classification to provide contextual information and context management. Simulation results show that the proposed object classification is useful to improve network lifetime. Results also give motivation of object classification in terms of energy consumption. This paper also presents proof of concept and time analysis of the proposed decision theory based object classification.

General Terms  
Identity Management, Internet of Things

Keywords
Decision theory; Identity Management; Internet of Things; Object Classification

1. INTRODUCTION
Internet of Things (IoT) is an integral part of the future Internet where virtual and physical objects can communicate with other objects giving seamless service to other entities. The realistic notion of IoT introduced in [1] has been realized with the development of technologies such as handheld objects, sensors, wireless communication and mobile Internet access. The greater scale and scope of IoT enable a user to interact with the objects in his/her physical as well as virtual environment. This broader scope of interactions stresses the need to extend current privacy, security and identity management (IdM) models to include how users interact with the objects. To address IdM and access control in IoT, this paper presents a decision theory based object classification. The outcome of the object classification acts as an input for context management [2] to design effective policies for access control mechanisms. Objects, identities and interaction of the objects are three major components of IoT. In [3, 4], the authors addresses IdM technical issues in IoT including challenges and road map. Identity management with authentication and access control have also been addressed in [5, 6] in the context of IoT.

This paper is structured as follows: Section 2 presents the motivation for object classification and discusses different scenarios in IoT context. Section 3 focuses on the state of the art in object classification. Section 4 discusses the proposed decision theory based object classification and framework. Section 5 presents the proof of concept and results as well as discusses time analysis and adversary models. Section 6 discusses the simulation result. Finally, section 7 concludes the paper underlining the uniqueness and efficiency of the proposed solution.

2. MOTIVATION
When interacting with IoT-objects, the context of use (as delivered by embedded sensors, from the vicinity of the things, as well as from the users using it) and the types of objects plays an important role to determine, what the interaction is about. Access control is one of the key issues in IoT due to the distributed and ad-hoc nature of such systems. In IoT, an object will have to assume that arbitrary objects can establish direct, ad-hoc communication with it. Therefore, object classification and identification become key research issues to address [4]. Due to mobility and heterogeneity of tiny wireless objects communicating with each other, the problem of IdM is crucial [3-7] and it becomes very important to classify these objects with respect to operational capacity. Context and context aware computing were first introduced in [2] where the context was defined as properties related to any communication entity. The properties can be familiar ones such as mobility and size or type of the devices. The goal of context management is then to collect information and utilize this to avail positive impact on the provisioning of access control or other services for a particular IoT device. In this sense, context information is only useful if it can be interpreted. Bayesian inference, which is an objective method of induction, proves how contextual information is useful for designing effective access control rules with object classification. The result of the inference justifies that there is a need of contextual object classification in IoT [8]. From the inference given in [8], it can be seen that rather than depending upon network topology to classify objects, a decision rule needs to evolve to enforce context-based object classification. This paper presents an extension and application of our previous work with the simulation results, time analysis and adversary models [9].

The context information in terms of object classification is useful for designing effective policies and efficient access control mechanisms. Depending on the classification of objects; it is easy to apply appropriate access control rules. Objective of this paper is to include contextualization based on types of objects and to use this contextual information for improving access control. Object classification based context
management for IdM in IoT is the main contribution of this paper.

3. RELATED WORK

In the context of IoT, tag level object identification and classification based on Certification Authority (CA) is proposed in [10], which is not suited for IoT due to the centralized architecture and lack of scalability. A Bayesian approach for object classification is presented in [11], which is camera and image based and not suited for nomadic and mobile scenarios in IoT. An overview of decision theory for sensor management in view of information gathering is presented in [12]. Integration of various components of sensor networks using a decision theory approach is suggested in [13] with the proposal for sensors scheduling. Necessity of context awareness with tagging, presenting information and automatic execution is given in [14], but concrete implementation is unaddressed. Due to the lack of sufficient computational power, the expected level of context awareness could not be achieved for the architectural solution presented in [15]. The taxonomy of IoT devices is proposed in [16] based on the processing power to design appropriate architecture facilitating device orchestration. Algorithms and methods for device classification are not presented in [16], but more focus in architectural issues. An ontology based device classification is proposed in [17], but the performance and accuracy of the proposed solution is not addressed. Furthermore, adversary analysis of the proposed solution is not presented in [17]. Table 1 shows evaluation summary of the related work based on the parameters like security, time efficiency, multi-context and expected level of context awareness.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Security</th>
<th>Time Efficiency</th>
<th>Multi-Context</th>
<th>Level of Context Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Orchestration [10]</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>Tag Level Classification [11]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Good</td>
</tr>
<tr>
<td>Camera based Classification [16]</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td>Context Awareness with Tagging [12]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Average</td>
</tr>
<tr>
<td>Group Localization [17]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>Ontology based Classification [17]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Good</td>
</tr>
</tbody>
</table>

Table 1: Evaluation of the Related Work

Let \( \{w_1, w_2\} \) be the finite set of two states of objects. The state of an object includes classes or categories. Let, \( w = w_1 \) for expedient and \( w = w_2 \) for non-expedient objects. A decision is made about the object with only prior information as given in [18]:

\[
\text{Decision (object)} = \begin{cases} 
  w_1 & \text{if } P(w_1) > P(w_2) \\
  w_2 & \text{otherwise} 
\end{cases}
\]

\( x \) is introduced as the continuous random variable which represents the Transmit Receive Traffic (TRT). TRT in an IoT scenario is the number of objects communicating with a particular object. Based on the potential or capability of the object, the number of objects communicating with a particular object will vary. This factor also depends on the IoT scenario such as health, smart home or agriculture. TRT, as introduced here, can be easily extended to multiple features and multiple classes as well as multiple contexts.

Class conditional probability density is given by \( P(x | w_j) \) where \( j = 1, 2 \) which means that probability of \( x \) given that the state of nature is \( w_j \) for \( j = 1, 2 \). \([P(x | w_1)] \) and \([P(x | w_2)]\)
describe the difference in the lightness between the number of expedient and non-expedient objects. Lightness is a continuous random variable and to develop better rules, we must extract some features from the data. Since the object may communicate with any number of objects, let’s assume \( x = \{0, 4, 8, 12, 16, \ldots, 48\} \) (these values of \( x \) are used to calculate average \( Pa \) for Case I, II and II described below) and \( p(x \mid w_j) \) is given in equation (2).

\[
P(x \mid w_j) = \frac{P(x \cap w_j)}{P(w_j)} \tag{2}
\]

Where \( x \cap w_j \) represents the object with which \( w_j \) communicates. \( P(w_j) \) and \( P(x \mid w_j) \) for \( j = 1, 2 \) and measure for lightness of the object as the value \( x \) are known. Let \( P(w_j \mid x) \) be the posterior probability which means the probability of the state of nature being \( w_j \) given the measurement of feature value \( x \). Bayes formula \([19]\) is used to convert prior probability to posterior probability as:

\[
P(w_j \mid x) = \frac{P(x \mid w_j) P(w_j)}{P(x)} \tag{3}
\]

Where \( P(x) = \sum_{j=1}^{2} P(x \mid w_j) P(w_j) \) and \( P(x \mid w_j) \) is called the likelihood. Finally, based on the prior and posterior analysis, eq. 3 can be written in terms of \( w_1 \) and \( w_2 \) for the decision of object as

\[
\text{Decision (object)} = \begin{cases} 
  w_1 & \text{if } \frac{P(x \mid w_1)}{P(x \mid w_2)} > \frac{P(w_1)}{P(w_2)} \\
  w_2 & \text{otherwise}
\end{cases} \tag{4}
\]

Equations (1), (2), (3) and (4) along with Case I, II and III are used in simulation for the expedient object selection. These three cases are most probable scenarios cases for IoT and proposed approach is applied to object classification using the framework described below.

### 4.2 Proposed Framework for Object Classification

The proposed logical framework is depicted in Figure 1 and provides a security infrastructure upon which IoT services can be built. The figure gives a high-level overview of the various logical components that comprise authorization, authentication and access control and shows that the decision logic is acting as an input for each security component in terms of context management. When interacting with IoT objects, the context of use will play an important role to determine what the interaction relates to. The framework is needed to implement tight security control for the integration with IdM systems and the proposed decision theory based solution of object classification is vertically applicable to all requisites of IdM. An attacker needs to compromise context management with decision theory logic and, in turn, access control to affect the IdM. It is assumed that the physical security of devices is being handled by embedded security solutions. Compromising one of these components in the framework will not solve the purpose of adversary without gaining anything. The outcome of this contextual information is the policy definition language and the enforcement mechanism.

As decision theory results in a rational framework for object classification in case of uncertainty, the proposed framework shall develop general tools and decision rules. In particular, the objective is to provide access to resources and services to authorized users and objects. This is to be achieved without time-consuming and complex security policies and access control procedures.

### 5. PROOF OF CONCEPT AND TIME ANALYSIS

This section presents the proof of concept of the proposed decision theory based object classification.

#### 5.1 Proof of Concept

Considering the scenario where prior probabilities are known, let \( P(w_1) = 0.5 \), which implies that the next object is an expedient object, and \( P(w_2) = 0.5 \). Another assumption here is that there are no other types of objects present. This assumption implies the property of exclusivity as:

\[
P(w_1) + P(w_2) = 1 \tag{5}
\]

**Case I**

Case I indicates the prior probabilities where probability of object \( w_1 \) and \( w_2 \) is 0.5. Calculations for different values of \( P(x \mid w_1) \) and \( P(x \mid w_2) \) for different \( x \cap w_j \) give the average \( Pa \):

\[
\text{Average } Pa(x \mid w_j) = 1.04 \approx 1
\]

The average \( Pa \) is calculated by taking the average of all probabilities \( P(x \mid w_1) \) for different values of \( x = \{0, 4, 8, 12, 16, \ldots, 48\} \). Priori analysis of the equi-probable scenario of different values of \( P(x \mid w_1) \) and \( P(x \mid w_2) \) with \( x \cap w_j \) values is calculated. As this case represents equi-probable values for \( w_1 \) and \( w_2 \), \( P(x \mid w_1) \) and \( P(x \mid w_2) \) have the same value. Case I results in gaining confidence on the decision of the selection of object. Extending eq. (1) for
posterior analysis to get the probability of error for a given decision gives:

\[
P(\text{error} | x) = \begin{cases} P(w1 | x) & \text{if decide } w2 \\ P(w2 | x) & \text{if decide } w1 \end{cases}
\]

Bayes decision rule minimizes this error because:

\[
\text{P (error | x)} = \min \{ P(w1 | x), P(w2 | x) \}
\]

and posterior calculations for posterior probabilities as \( P(w1) = 0.5 \) and \( P(w2) = 0.5 \) shows that \( P(\text{error}) = 0.5 \). Decision (object)' = w1 and, hence, it concludes that Decision (object)' from posterior strongly proves aforementioned prior decision result.

**Case II**

In case II, the scenario where the prior probabilities are \( P(w1) = 0.8 \) and \( P(w2) = 0.2 \) is considered. Calculations for class conditional probability density give:

\[
\text{Average } P_a(x | w1) = 0.671 < 1
\]

As per eq. (2), \( P(w1 | x) = 0.50074 \) and \( P(w2 | x) = 0.5 \), hence eq. (5) holds true justifying case II. As per eq. (4), Decision (object)' = w1.

**Case III**

In case III, the scenario where the prior probabilities are \( P(w1) = 0.3 \) and \( P(w2) = 0.7 \) is considered. Calculations for class conditional probability density give:

\[
\text{Average } P_a(x | w2) = 0.7575 < 1
\]

As per eq. (2), \( P(w1 | x) = 0.50 \) and \( P(w2 | x) = 0.49 \), hence eq. (5) holds true justifying case III. As per eq. (4), Decision (object)' = w1.

Priori analysis of case III for the different values of \( P(x | w_1) \) and \( P(x | w_2) \) with \( x \) \( w_j \) values is similar to the case where \( w1=0.3 \) and \( w2=0.7 \). This is the case where public or private IoT contains more non expedient object than expedient objects. Proof of concept shows that decision theory based solution is useful in expedient object selection correcting the priori analysis in uncertainty.

**5.2 Time Analysis**

The procedure for BDT in identifying the expedient object or non-expedient object is divided into broadly three phases. The first phase is Priori Analysis, class conditional probabilities and Posterior Analysis. First phase has the unit time complexity as the implementation involves single instruction executions (conditional or arithmetic). Next phase involves computation of class conditional probabilities these probabilities are dependent upon the value of no. of the feature element which is considered to be of size ‘b’. ‘b’ features represent the traffic i.e. property over the network. Last phase involves a posterior computation which depends on class conditional probabilities. Again this phase involves single instruction executions.

Above mentioned is single iteration computation for say unit input. Let the input size say 2 i.e. for \( w1 \) and \( w2 \). This results in the following recurrence relation for time complexity as given in equation (7).

\[
T_n = \begin{cases} 1 & \text{if } n = 0 \text{ or } 1 \\ b & \text{if } n = 2 \\ T_{n-1} + b & \text{if } n > 2 \end{cases}
\]

Solving this recurrence equation yields \( T_n \) as \( T_n \sim (b)^{n-1} \).

Hence, it is concluded that the proposed solution has the time complexity of the order of \( O(b)^{(n-1)} \), where \( b \) is the size for the set of the feature element ‘x’ and at some time t, it is small giving efficient scenario dependent time complexity. These results are based on the calculations for three cases described above. Average values of \( P_a(x | w_j) \) are given in respective cases. This results in gaining more confidence on the decision of the selection of the object. Hence it proves that BDT is efficient in expedient object selection correcting the priori analysis.

**5.3 Adversary Models**

Proposed solution of object classification for IdM needs to be analyzed for adversary models. Adversary is classified based on their capabilities like nature as active or passive, static or adaptive, computational ability, mobility and byzantine. Adversary models are subject to change depending on the underline application. Adversaries are classified based on their capacities into three types as

1) **Weak Passive**: Passive eavesdropper with limited capacity and cannot gain whole control over transmission path
2) **Strong Passive**: Passive eavesdropper and can gain whole control over transmission path
3) **Strong Active**: Active eavesdropper with the ability of compromising intermediate source and destination

Logical framework in Figure 1 shows that proposed decision theory based solution of object classification is vertically applicable to all requisites of IdM. Strong Active type of adversary which is the most powerful, needs to compromise context management with decision theory logic in turn access control to affect IdM. It is assumed that physical security of devices is being taken care by embedded security solutions. Compromising one of these will not solve the purpose of adversary without gaining anything.

**6. SIMULATION RESULTS AND DISCUSSION**

Functionalities and operatonal principle of Wireless Sensor Networks (WSN) makes it appropriate and mandatory candidate of IoT. Simulation is carried out in NS2 and IoT scenario is simulated by assigning different energy levels of mobile nodes. 100 mobile nodes are deployed in the area of 800*800 meters. Initial energy is set as 50 Jules for the full energy nodes and 2o Jules for the less energy nodes. Transmission and receiving power is set as 0.6 mW and 0.3 mW respectively with 0.01 meter / second as node speed. The factor TRT is introduced in simulation in terms of number of connections which are in the range of 30, 40 and 50. Simulation time is 500 sec with the packet interval of 0.05 seconds. Energy Consumption Ration (ECR) is introduced as
new performance parameter in this paper and given in equation (8) as:

\[
ECR(\%) = 100 - \left( \frac{\text{Remaining Energy}}{\text{Initial Energy}} \right) \times 100
\]  

(8)

Simulation is run with the variable number of traffic as 30 and 40 where number of traffic represents number of source and destination pair. If no. of traffic increased no of data transmission and reception also increases. Percentage of full energy node is varied from 10 to 90 and ECR for full energy as well as less energy nodes is measured. Simulation results are shown in figure 2.

Figure 2 shows simulation results for the number of traffic = 30 & 40. The of simulation show that ECR is high for the nodes with low energy and ECR is low for the nodes with high energy. This is very important observation from Figure 2, as classifying object into two types as expedient and non-expedient (high energy and low energy respectively) helps to get useful context information as well as expedient object gives less ECR. This is indeed very useful simulation result where object classification helps for context management inorder to apply proper access control mechanism for IdM to achieve less ECR.

Case I, Case II and Case III are generalized in the simulation results shown in Figure 3 and 4. This simulation is also conducted for number of traffic = 30 & 40. These cases are generalized for expedient and non-expedient objects by varying percentage (%) of full energy nodes. Figure 3 shows the simulation result of % full energy nodes versus packet delivery ratio (PDR). Figure 3 shows that PDR is the minimum for 50 % of the full energy nodes which is case of equi-probable probabilities, where \( w_1 = 0.5 \) and \( w_2 = 0.5 \).This result depict that PDR is high for IoT scenario in which expedient objects are more i.e. objects with high energy and this context information is very useful do design effective policies of access control in order to achieve IdM.

In our analysis, we took energy parameter as a classification parameter. The number of less energy (non-expedient) and number of high energy (expedient) nodes impact the network behavior. If number of less energy node increased we require proper object classification and access control method to increase the network lifetime. An ontology-based device classification depending on the data coming is presented in [17]. In this approach, a complete match is carried out to fetch device type and provider from the database. Reliability is not proved with even the proof of concept in this approach. Communication cost in terms of energy, PDR is also not addressed in [17].
7. CONCLUSIONS AND FUTURE WORK

Confronting uncertainty of varied types of objects in IoT is a challenging issue. This paper has presented the logical framework for object classification in order to provide contextual information. Proposed solution and framework for object classification is the time efficient and scalable. The objective is a selection problem with two object considered from a partially defined set. The set which comprises objects based on the property of likeness of being expendient or non-expendient. Results show an optimization on binding the posterior value on expendient item and, thus are making the selection procedure proficient. Paper shows that when presented with the worst-case scenario it is proposed to select the object which has got a strong feature value which in our case is the expendient object. Hence, the selection made is of the object of use and reject non expendient object so that process access control can be in place to achieve IdM. Simulation results show that the proposed object classification is useful to improve network lifetime. Results also give motivation of object classification in terms of energy consumption.

Future plan is to use this mathematical model, framework and results for capability based access control in IoT.

8. REFERENCES


