Prétopologie et protection de la vie privée dans l'Internet des Objets

Pretopology and privacy protection in the Internet of Things

Amri Toumia[1], Samuel Szoniecky[2]

[1] Laboratoire Paragraphe EA 349, Université Paris VIII, Saint-Denis France, amri.toumia@etud.univ-paris8.fr
[2] Laboratoire Paragraphe EA 349, Université Paris VIII, Saint-Denis France, samuel.szoniecky@univ-paris8.fr

RÉSUMÉ. L'article présente un moyen de représenter la vie privée à travers des diagrammes, ceci dans le cadre de l'Internet des Objets. En utilisant la prétopologie, nous étudions comment créer une organisation graphique et conceptuelle de la vie privée qui peut permettre son paramétrage par manipulation des éléments graphiques du diagramme. Dans la première partie de cet article, nous définissons ce qu'est la vie privée et nous évoquons des travaux importants qui traitent de ce sujet. Nous présentons, ensuite, quelques concepts de la prétopologie et nous détaillons l'intérêt de son utilisation pour notre modélisation. En deuxième partie, nous étudions la modélisation de la vie privée dans l'Internet des Objets en prenant comme exemple celui d'une montre intelligente. Nous concluons enfin en évoquant les futurs travaux à partir de cet article.

ABSTRACT. The article presents a way to represent privacy in the context of the Internet of Things via diagrams. Using pretopology, we study how to create a graphical and conceptual organization of privacy that can allow its parameterization by manipulation of the graphical elements of the diagram. In the first part of this article, we define what privacy is and we present important work that deals with this topic. Then, we present some concepts of pretopology and we detail the interest in using it for our modelling. In the second part, we study the modelling of privacy in the Internet of Things by using the example of a smart watch. Finally, we conclude by discussing future work from this article.

MOTS-CLÉS. Vie privée, Internet des Objets, modélisation, prétopologie.
KEYWORDS. Privacy, Internet of Things, modelling, pretopology.

1. Introduction

Nous vivons dans un monde de plus en plus connecté où on génère et crée de plus en plus de données de nature différente. À cause des réseaux sociaux, du Big Data et maintenant avec l'émergence de l'Internet des Objets (IoT : *Internet of Things*), une quantité énorme de données personnelles est mise en jeu et divulguée parfois même sans que les intéressés en soient conscients. Face à ce risque de sécurité et ce problème de protection de la vie privée, de nombreux chercheurs se sont penchés sur cette thématique de privacy ou de protection de la vie privée. Différentes approches ont été proposées, notamment celles qui se basent sur des techniques de cryptographie, qui s'avèrent compliquées à comprendre pour un simple utilisateur, ou bien celles qui mettent en place des systèmes de contrôle d'accès et d'autorisation, qui, quant à elles, ne s'avèrent pas évidentes à configurer.

L'objectif de cet article est de poser plusieurs hypothèses concernant la protection de la vie privée dans l'IoT et son paramétrage. Pour cela, nous allons prendre comme cas pratique l'Internet des Objets et l'exemple d'une montre intelligente possédant des capteurs qui mesurent différents paramètres se rapportant à l'utilisateur. Par le biais de la prétopologie, peut-on créer une organisation graphique et conceptuelle de la privacy et permettre ainsi son paramétrage par manipulation des éléments graphiques d'un diagramme ?

Dans ce qui suit, nous consacrerons la première partie de notre article à définir la privacy et nous évoquerons d'autres travaux importants qui traitent de la protection de la vie privée. Nous passerons par la suite à la définition de la prétopologie et nous détaillerons l'intérêt de son utilisation pour notre

modélisation. En deuxième partie, nous nous pencherons sur la possibilité de modélisation de la privacy en prétopologie et les intérêts que cela peut avoir. Nous terminerons enfin par un résumé de notre étude et nous parlerons de nos travaux futurs à partir de ce papier.

2. Internet des Objet et vie privée

La protection de la vie privée est un sujet sur lequel les avis sont partagés. En effet, certains pensent que la privacy est un vieux problème qui n'est plus d'actualité dans notre contexte actuel de réseaux sociaux où on exhibe de plus en plus ses activités et ses idées[1]. D'autres estiment que la privacy n'est pas nécessaire si on n'a rien à cacher. D'un autre côté, les partisans de la protection de la vie privée la considère comme un droit fondamental et sa perte conduirait à la restriction de la liberté de l'individu[2].

Dans ce contexte, les législateurs planchent sur l'élaboration de lois pour fixer un cadre juridique à la vie privée. Le parlement européen, par exemple, s'est saisi de ce problème pour, à la suite des débats en cours, légiférer sur ces questions[3]. En effet, la protection de la vie privée qui est un droit fondamental pour tout individu (voir par exemple l'article 12 de la déclaration universelle des droits de l'Homme), continue d'être un des sujets de discussions du parlement européen. Cependant, la privacy reste une notion difficile à définir et à formaliser à cause de la complexité des contextes qu'il faut prendre en compte.

Mais qu'est ce que la protection de la vie privée et que doit-on protéger ? Selon Brandeis et Warren [WAR 90], la privacy est définie comme « le droit d'être laissé tranquille » (*right to be left alone*). Dans les travaux de Alan Westin [WES 68], la privacy est « le droit des individus, des groupes ou des institutions à décider pour eux même quand, comment et dans quelle mesure une information les concernant est communiquée à autrui ». La déclaration universelle des droits de l'Homme[4] stipule que « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

Il y a donc des différences importantes entre ces définitions. D'un côté, Westin se focalise plutôt sur l'accès à l'information et comment une information devient connue. D'un autre côté, la déclaration des droits de l'Homme et la définition de Brandeis et Warren se concentrent sur ce qui arrive aux individus lorsque des informations les concernant sont utilisées. Les discussions actuelles sur la privacy, que ce soit sur les politiques de vie privée ou des technologies de protection, ont tendance à prendre le point de vue de Westin. La focalisation sur le contrôle d'accès considère parfois la privacy et les données personnelles comme une sorte de « monnaie de l'ère digitale » que les utilisateurs peuvent échanger contre de meilleurs résultats de recherche ou des services plus personnalisés.

L'Internet des objets (IoT) est un nouveau concept qui désigne des appareils interconnectés, des systèmes et des services qui reposent sur une communication autonome entre les objets physiques au sein de l'existante infrastructure Internet. Ceci permet d'apporter les connaissances d'Internet à des objets physiques, les rendant ainsi capables de communiquer et d'échanger des données dans le cadre de différents domaines d'application, comme par exemple, la santé, l'environnement, le transport, l'industrie et les loisirs [LI 15]. Le développement de l'IoT entraîne avec lui une redéfinition des frontières du numérique [BOU 16] qui impacte fortement nos sociétés sur le plan technique, industriel, économique, social et politique [SZO 17, SAL 17].

[1] http://www.internetactu.net/2009/03/12/la-vie-privee-un-probleme-de-vieux-cons/

[2] https://robindoherty.com/2016/01/06/nothing-to-hide.html

[3] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0005&format=XML&language=FR

[4] http://www.un.org/fr/universal-declaration-human-rights/

Dans l'IoT, l'environnement est mesuré et analysé à l'aide de capteurs et d'appareils connectés. Les informations recueillies sont ensuite envoyées à un serveur qui contient la logique applicative. Dans ce contexte, la privacy doit être assurée au sein des appareils connectés, durant le stockage, la transmission et le traitement de l'information [BAR 16]. En effet, la sécurité des données et la protection de la vie privée ont été identifiées comme l'un des problèmes majeurs de l'IoT, et représentent l'un des freins importants à son adoption [BER 16].

Pour résoudre ce problème, nombreux scientifiques se sont penchés sur la question. On peut donc trouver dans la littérature, de nombreux travaux portant sur la protection des données et de la vie privée dans l'IoT. Les solutions proposées portent sur la protection des données transmises vers le « cloud » [LI 13] [HEN 14] [POO 14]. D'autres auteurs se sont penchés sur la protection des données par des mécanismes de cryptographie adaptés à un environnement IoT caractérisé par une faible puissance de calcul comme [SHA 15] [KOT 16], [SAL 16] pour en citer quelques-uns. Par ailleurs, il existe aussi d'autres travaux qui portent sur la protection de la privacy des utilisateurs dans l'IoT par la définition de politiques de vie privée et des préférences de protection. Ainsi, Davies et al. [DAV 16] ont développé ce qu'ils appellent un « *privacy mediator* ». Basé sur la technologie des « *cloudlets* », leur système consiste en un module qui est inséré dans le pipeline de distribution des données. Il réalise l'agrégation et l'obfuscation des données et aide à l'application des politiques de protection de vie privée mises en place, ceci avant que les données soient libérées du contrôle de l'utilisateur pour être envoyées sur le cloud. Aussi, Neisse et al. ont proposé *SecKit* [NEI 15], un framework appliqué au cas d'une ville intelligente, plus particulièrement les interactions entre une maison intelligente, un véhicule intelligent et un bureau intelligent. La partie principale de la solution proposée est un outil de contrôle, où les politiques de protection de la vie privée peuvent être utilisées pour réguler l'accès aux données et aux ressources dans l'IoT, ceci avec la possibilité de supporter le changement dynamique de contexte. Enfin, Chen et al. ont développé CoBrA (Context Broker Architecture) [CHE 04], un framework qui prend en compte l'aspect sécurité et vie privée dans l'IoT. Il est utilisé pour le cas de salle de réunion intelligente, où la confidentialité des données qui y sont échangées ainsi que la protection de la vie privée des participants sont une priorité. Leur article souligne aussi la difficulté de protéger la vie privée quand le contexte change dynamiquement et que les utilisateurs doivent manuellement définir leurs politiques de protection de vie privée pour chaque contexte.

On remarque que, pour la protection de la vie privée des utilisateurs dans l'IoT basée sur la définition des politiques et des préférences en matière de privacy, les usagers se retrouvent souvent perdus face à la complexité du système et n'arrivent pas à concevoir les répercussions de partager leurs informations sur leurs vies privées. Dans ce cadre, la prétopologie peut être un outil pratique pour permettre aux utilisateurs de définir leurs préférences en matière de vie privée et mieux contrôler la diffusion de leurs informations grâce à des outils visuels.

2.2. *Prétopologie : définitions et usages*

La prétopologie résulte principalement des travaux d'un groupe de chercheurs qui s'est intitulé Z. Belmandt [BEL 93] et qui cherchait à réduire la complexité axiomatique de la topologie ensembliste ou générale. Pareillement que la topologie, la prétopologie traite des questions de proximité, de voisinage, sans rapporter ces notions à l'usage d'une distance. En effet, l'opérateur qui structure la prétopologie n'est pas la distance, mais un opérateur élémentaire tout en étant général qui associe à une partie son extension.

La prétopologie peut être considérée comme un outil mathématique de modélisation du concept de proximité pour les systèmes complexes. Parmi les perspectives d'applications offertes par la prétopologie et ses concepts de proximité, on peut citer [AUR 09] :

– « *la théorie des graphes et un certain nombre d'applications dans le domaine de la formation de groupes sociaux* »,

– « *certains aspects de la théorie des jeux comme ceux qui portent sur le problème de formation de coalitions* »,

– « *des méthodes de classification utilisables sur des ensembles dotés simplement de structure prétopologique et non pas de structure métrique* ».

Jusqu'à présent, gérer des ensembles munis d'un nombre fini, mais élevé d'objets a été un obstacle à l'utilisation de l'outil prétopologique. « *Mais le développement des moyens de calcul combiné avec la construction d'algorithmes adaptés rend désormais réalisables des applications à des problèmes concrets.* » [AUR 09]

« *La prétopologie permet le développement de technologies intéressantes pour une raison essentielle : sa souplesse pour assurer le suivi, pas à pas, de processus de description et de transformation d'un ensemble. Ceci correspond très bien aux concepts de l'informatique pour la modélisation et la simulation de phénomènes complexes. Des développements informatiques innovants, notamment la librairie PRETOPOLIB* [LEV 10a]*, permettent désormais de manipuler aisément les concepts de la prétopologie et de réaliser des applications en mesure de traiter des collections de données de grande taille, proposant ainsi un outil pédagogique, mais également son usage pour la simulation et le prototypage d'applications ».* [AUR 09]

Nous allons maintenant rappeler quelques concepts prétopologiques à partir de l'article de [LEV 10b] :

Adhérence :

Une application $a(.)$ de $P(E)$ à $P(E)$ est appelée *adhérence* si et seulement si $\forall A \in P(E)$:

1. $a(\varnothing) = \varnothing$
2. $A \subset a(A)$

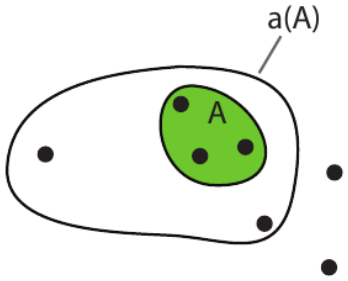

Figure 1. *Adhérence de A (source [LEV 10b])*

Intérieur :

On définit l'application *intérieur* par dualité comme suit :
Soit une adhérence $a(.)$ sur E, l'application intérieur est définie par :

$$\forall B \in P(E), i(B) = C.a.C(B) \qquad [1]$$

où $C(B)$ est le complémentaire de la partie B c'est-à-dire E-B

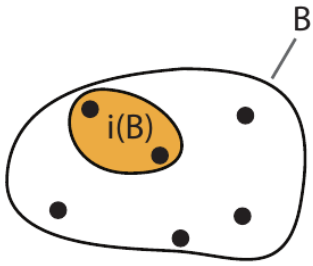

Figure 2. *Intérieur de B (source [LEV 10b])*

La relation d'inclusion entre i(A) et a(A) peut être définie comme suit :

$$\forall A \in P(E), i(a) \subseteq A \subseteq a(A) \quad [2]$$

Proche, lointain, intermédiaire :

La prétopologie définit aussi l'extérieur d'une partie par le complémentaire de son extension :

$$\forall A \in P(E), ex(A) = C.a(A) \quad [3]$$

L'extérieur est composé d'éléments qui peuvent être considérés comme éloignés de la partie. À l'inverse de l'intérieur, où les éléments s'y trouvant sont considérés comme étant proches les uns des autres.

Entre l'intérieur et l'extérieur se trouve la frontière qui est composée de deux parties : le bord et l'abord. Le bord d'une partie, l'abord et la frontière sont définis comme suit :

$$\forall A \in P(E), b(A) = A \cap a.C(A) \quad [4]$$

$$\forall A \in P(E), ab(A) = a(A) \cap C(A) \quad [5]$$

$$\forall A \in P(E), \delta = b(A) \cup ab(A) \quad [6]$$

D'après l'article de Serge Thibault [THI 17], la prétopologie permet de manipuler des concepts de proximité dans des ensembles où il n'est pas possible d'appliquer une métrique traditionnelle. En effet, grâce à la définition de l'intérieur, de la frontière et de l'extérieur, la prétopologie propose trois états liés à la relation proche/lointain. Selon lui, pour chacune des parties de l'ensemble des parties, le proche est constitué des éléments qui sont au sein de la partie, c'est à dire, qui composent son intérieur. Les éléments lointains sont au-delà de son extension. Entre le proche et le lointain se trouvent les éléments de la frontière qui sont considérés comme intermédiaires.

Dans la troisième partie, nous verrons l'intérêt de la notion de proximité dans la définition graphique de la vie privée et nous détaillerons cela par des exemples.

Espace prétopologique :

On définit le triplet (E,i,a) comme étant un espace prétopologique.
À partir de ces propriétés, on obtient des espaces prétopologiques plus ou moins complexes, du général jusqu'à l'espace topologique. Les espaces les plus intéressants appartiennent au type V. Ceux-ci possèdent la propriété suivante :

$$\forall A \in P(E), B \in P(E), A \subseteq B \Rightarrow a(A) \subseteq a(B) \quad [7]$$

Fermeture : Le processus de dilatation (cf. figure 3) généré par l'adhérence s'arrête à un instant donné et n'évolue plus. Dans ce cas, on a :

$$\forall A \in P(E), a^{k+1}(A) = a^{k}(A) \text{ avec } k \in \mathbb{N} \quad [8]$$

On nomme A comme étant un sous-ensemble fermé.
De la même manière, l'évolution de l'intérieur va cesser, ce qui donne :

$$\forall A \in P(E), i^{k+1}(A) = i^{k}(A) \quad [9]$$

Cette fois, on nomme A comme étant un sous ensemble ouvert.
Respectivement, on utilise les notations F(A) pour la fermeture de A et O(A) pour l'ouverture de A.

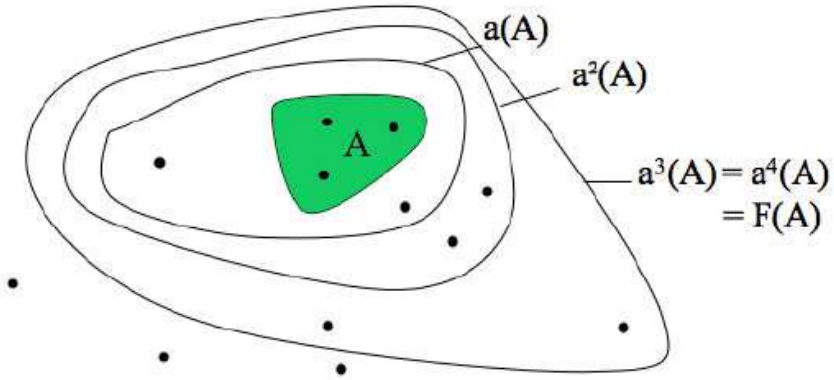

Figure 3. *Adhérences successives de A menant au fermé (source [LEV 10b])*

3. Prétopologie et vie privée

Dans cette partie, nous allons étudier la possibilité d'utiliser la prétopologie pour modéliser la privacy et plus particulièrement la privacy dans le cas de l'Internet des Objets (IoT). Pour cela, nous allons prendre comme cas d'utilisation celui d'une montre intelligente. Cette dernière permet de mesurer la pression sanguine (PS), la fréquence cardiaque (FC), la température (T) et la localisation géographique (Lo) d'un utilisateur.

Considérons un ensemble E constitué des espaces mémoires des appareils et acteurs du monde numérique. Une partie de cet ensemble peut être constituée par les espaces de stockage de ces entités. Dans le cas de la privacy, il serait intéressant d'étudier la diffusion ou non d'une information d'un espace mémoire vers un autre. Ainsi, le processus d'adhérence pourrait être celui qui associe l'espace mémoire d'une entité à une autre suivant la diffusion (ou la copie) d'une information donnée.

Considérons dans un premier temps, un exemple où l'utilisateur partage ses informations sur la PS et FC avec la plateforme IoT. Comme décrit précédemment, le processus d'adhérence représente le partage d'une information d'un espace mémoire à un autre.

On a donc $M = (PS, FC, T, Lo)$ qui représente l'ensemble des mesures de la montre intelligente enregistré dans son espace mémoire. L'adhérence de M, *a(M)* revient à ajouter les espaces mémoire de la plateforme IoT où seront stockées *PS* et *FC* à la partie *M*. Donc :

$$a(M) = (PS, FC, T, Lo, PS_1, FC_1) \quad [10]$$

avec PS_1 et FC_1 les espaces mémoire de la plateforme IoT qui recevront les informations *PS* et *FC* partagées par l'utilisateur.

L'intérieur de M :

$$i(M) = C.a.C(M) = C.a(E-M) = C(E-M) = M \quad [11]$$

Quant à l'extérieur de la partie M, noté *ex(M)*, il est comme suit :

$$ex(M) = C.a(M) = E - a(M) \quad [12]$$

Le bord de la partie M, noté *b(M)* est :

$$b(M) = M \cap a.C(M) = M \cap a(E-M) = M \cap (E-M) = \varnothing \quad [13]$$

L'abord de M est :

$$ab(M) = a(M) \cap C(M) = (PS_1, FC_1) \quad [14]$$

La frontière de M est :

$$\delta = b(M) \cup ab(M) = (PS_1, FC_1) \quad [15]$$

Nous aurons donc la représentation décrite par la figure 4.

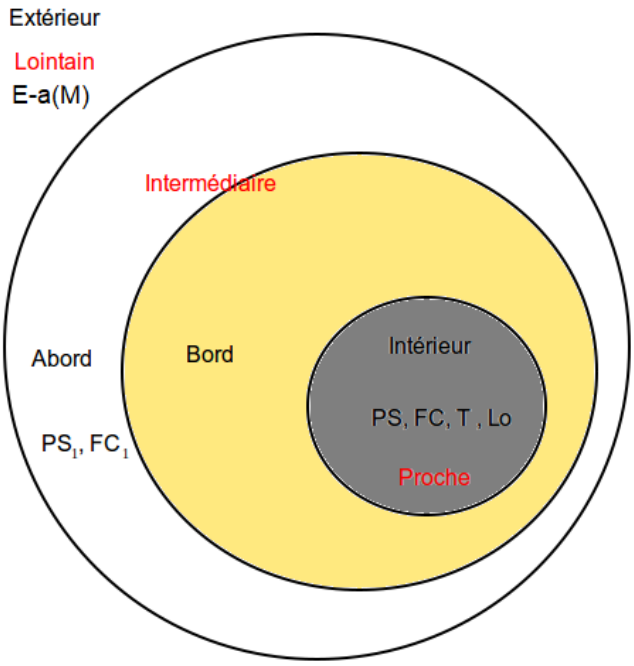

Figure 4. *Représentation topologique du partage d'information*

Dans ce schéma, on peut remarquer qu'on arrive facilement à représenter les notions d'intérieur, de frontière et d'extérieur. On voit que l'intérieur de la partie représente les informations sur l'utilisateur recueillies par la montre intelligente. En partageant ses informations avec la plateforme IoT de son objet connecté, l'utilisateur effectue une extension de son espace mémoire en intégrant l'espace mémoire de la plateforme IoT où seront stockées les informations partagées.

Dans cet exemple, « *le proche est constitué des éléments qui sont au sein de la partie, plus précisément qui constitue son intérieur* » [THI 17]. Ici, l'intérieur contient les mesures faites par la montre et qui sont stockées dans sa mémoire. « *Les éléments lointains sont ceux au-delà de son extension* » [THI 17]. Dans notre cas, le lointain représente les espaces mémoires de l'ensemble E sans ceux de la montre et de la plateforme IoT où seront stockés les informations que l'utilisateur partage. Entre le proche et le lointain, la frontière constituée du bord et de l'abord, représente ce que le processus d'extension ajoute à la partie en l'occurrence les espaces mémoire de la plateforme IoT où seront stockées les informations. Ces espaces mémoire sont donc créés grâce aux données générées par l'utilisateur. Cependant, elles n'appartiennent plus qu'à lui, mais aussi à la plateforme IoT.

Supposons maintenant que la plateforme avec laquelle l'utilisateur a partagé ses données les partage à son tour avec une partie tierce. Celle-ci peut être un publicitaire qui grâce aux données de localisation proposera un contenu plus ciblé ou bien une assurance qui pourrait adapter ses prix en fonction du mode de vie des utilisateurs. Bien sûr, selon les nouvelles lois sur la protection de la vie privée, la plateforme est obligée d'informer l'utilisateur de la transmission de ses données à une partie tierce et a aussi le devoir de spécifier l'objectif de leurs collectes.

On aura donc, comme nous l'avons décrit plus haut, un processus de dilatation de M à cause de l'application successive de l'adhérence, ou en d'autres termes à la transmission d'informations d'un acteur à un autre. La transmission des données de l'utilisateur à la partie tierce via la plateforme IoT peut se modéliser en prétopologie de la manière suivante :

$$a^2(M) = a(a(M)) = a(PS, FC, T, Lo, PS_1, FC_1) = (PS, FC, T, Lo, PS_1, FC_1, PS_2, FC_2) \quad [16]$$

Nous aurons donc la représentation visuelle suivante :

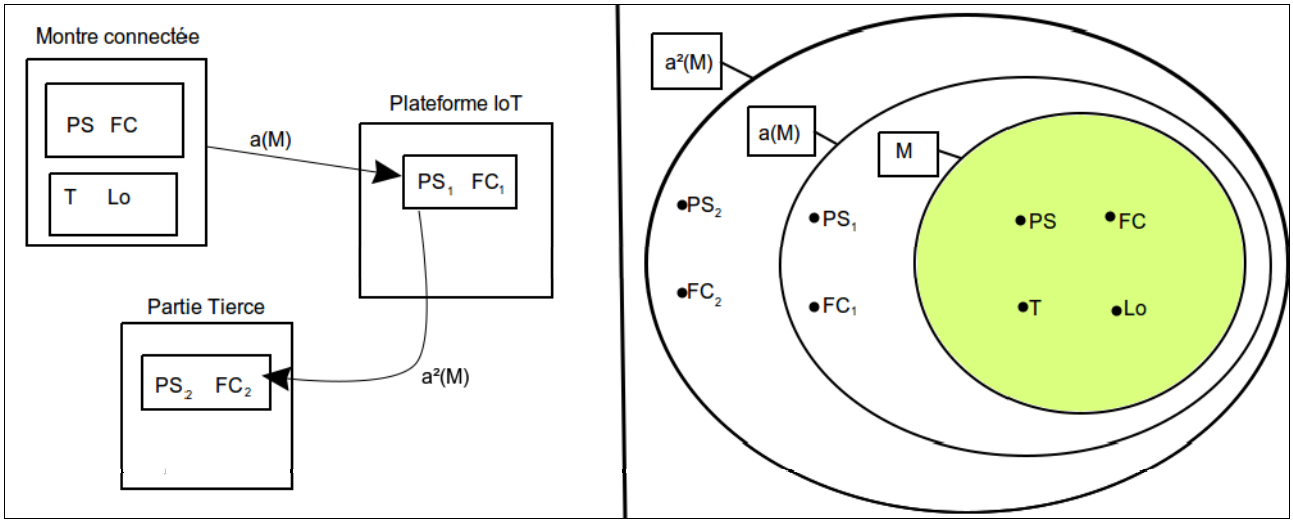

Figure 5. *Dilatation de M*

Grâce à cette représentation, un utilisateur peut observer la dilatation de ses informations et leurs propagations. On pourrait donc, à partir de la prétopologie et avec la libraire PRETOPOLIB, implémenter une représentation interactive qui indiquerait l'étendue des partages d'un objet connecté. Par ce biais, l'utilisateur aurait plus conscience des entités interagissant avec ses données. Par la suite, il pourrait, en modifiant un paramètre, changer ses préférences de privacy plus facilement et restreindre l'accès à ses données.

4. Conclusion :

Nous avons exposé dans ce papier ce que pourrait apporter la prétopologie à la modélisation de la privacy. Nous avons vu que, grâce au concept d'adhérence, on peut modéliser le partage d'une

information ou bien l'autorisation d'y accéder. Grâce à sa définition du concept de proximité, la prétopologie nous permet d'avoir une représentation graphique du partage d'information. Cette représentation peut être la base d'un système visuelle de paramétrage de la privacy. Grâce à ce dernier, l'utilisateur définira plus facilement ses préférences et aura une meilleure idée de l'impact de ses choix sur l'accès à ses données personnelles.

Dans nos futurs travaux, nous allons approfondir notre étude sur la représentation de la transmission de données dans l'IoT et leurs modélisations en prétopologie. Nous utiliserons ensuite la libraire PRETOPOLIB pour réaliser nos modélisations. Nous chercherons aussi à analyser les politiques de vie privée de quelques plateformes IoT afin d'identifier ce qu'elles recueillent comme informations et dans quels buts, ainsi qu'à quelles autres entités elles les transmettent afin de réaliser une modélisation plus détaillée. Nous espérons qu'à partir de cela, l'utilisateur pourra configurer plus facilement ses préférences de privacy et aura plus conscience de l'impact du partage de ces données avec une entité.

5. Bibliographie :

[AUR 09] Auray J.-P., Bonnevay S., Bui M., Duru G., Lamure M., "Prétopologie et applications: un état de l'art.," Stud. Inform. Univ., vol. 7, no. 1, pp. 25–44, 2009.

[BAR 16] Barki A., Bouabdallah A., Gharout S., Traore J., « M2M Security: Challenges and Solutions », IEEE Commun. Surv. Tutorials, vol. 18, no. 2, pp. 1241–1254, 2016.

[BEL 93] Belmandt Z., « Manuel de prétopologie et ses applications: sciences humaines et sociales, réseaux, jeux, reconnaissance des formes, processus et modèles, classification, imagerie, mathématiques », Hermes, 1993.

[BER 16] Bertino E., « Data Security and Privacy in the IoT », Proc. 19th Int. Conf. Extending Database Technol., pp. 1–3, 2016.

[BOU 16] Bouhaï N., Saleh I., Hachour H., Frontières numériques et artéfacts. Editions L'Harmattan, 2016.

[CHE 04] Chen H., Finin T., Joshi A., Kagal L., Perich F., Chakraborty D., « Intelligent agents meet the semantic Web in smart spaces », IEEE Internet Comput., vol. 8, no. 6, pp. 69–79, 2004.

[DAV 16] Davies N., Taft N., Satyanarayanan M., Clinch S., Amos B., « Privacy Mediators : Helping IoT Cross the Chasm », Proc. 17th Int. Work. Mob. Comput. Syst. Appl. - HotMobile '16, pp. 39–44, 2016.

[HEN 14] Henze M., Bereda S., Hummen R., Wehrle K., « SCSlib: Transparently Accessing Protected Sensor Data in the Cloud », Procedia Comput. Sci., vol. 37, pp. 370–375, 2014.

[KOT 16] Kotamsetty R., Govindarasu M., « Adaptive Latency-Aware Query Processing on Encrypted Data for the Internet of Things », in 2016 25th International Conference on Computer Communication and Networks (ICCCN), pp. 1–7, 2016.

[LEV 10a] Levorato V., Contribution à la Modélisation des Réseaux Complexes : Prétopologie et Applications, Thèse de doctorat, Université de Paris VIII Saint Denis 2010.

[LEV 10b] Levorato V., « Une méthode mixte d'analyse d'un réseau social: classification prétopologique et centralité d'intermédiarité », pp. 5–77, 2010.

[LI 13] Li M., Yu S., Zheng Y., Ren K., Lou W., « Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption », IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[LI 15] Li S., Da Xu L., Zhao S., « The internet of things: a survey », Inf. Syst. Front., vol. 17, no. 2, pp. 243–259, 2015.

[NEI 15] Neisse R., Steri G., Fovino I. N., Baldini G., « SecKit: A Model-based Security Toolkit for the Internet of Things », Comput. Secur., vol. 54, pp. 60–76, 2015.

[POO 14] Pooja B., Manohara Pai M. M., Radhika M.P., « A Dual Cloud Based Secure Environmental Parameter Monitoring System: A WSN Approach », Springer, Cham, pp. 189–198, 2014.

[SAL 16] Al Salami S., Baek J., Salah K., Damiani E., « Lightweight Encryption for Smart Home », in 2016 11th International Conference on Availability, Reliability and Security (ARES), pp. 382–388, 2016.

[SAL 17] Saleh, I., 2017. « Les enjeux et les défis de l'Internet des Objets (IdO) », Revue « Internet des objets » 1. DOI:10.21494/ISTE.OP.2017.0133

[SHA 15] Shafagh H., Hithnawi A., Droescher A., Duquennoy S., Hu W., « Towards Encrypted Query Processing for the Internet of Things », in Proceedings of the 21st Annual International Conference on Mobile Computing and Networking - MobiCom '15, pp. 251–253, 2015.

[SZO 17] Szoniecky S., Safin S., « Modélisation éthique de l'Internet des Objets », Internet des objets, vol. 17, no. 2, 2017.

[THI 17] S. Thibault, « Prétopologie et espaces habités », EspacesTemps.net, 2017.

[WAR 90] Warren S. D., Brandeis L. D., « The Right to Privacy », Harv. Law Rev., vol. 4, no. 5, pp. 193–220, 1890.

[WES 68] Westin A., « Privacy and freedom . New York, USA: Athenaeum », 1968.

