A Trust Secure Funnel based Mobile Service Discovery and Exposure Model

Walid El Ayeb
Higher School of Communications of Tunis
Mediatron Lab
Tunis, Tunisia

Zied Choukair
Higher School of Communications of Tunis
Mediatron Lab
Tunis, Tunisia

***Abstract*— IMS (IP Multimedia Subsystem) is confronted to various evolutions. The purpose of these evolutions is mainly to enhance subscriber experience by offering a variety of services that meets his needs and requirements. This variety of services and features involves interactions between different actors such as operators, service providers and subscribers. A meaningful mass of information within networks will be exchanged between these actors. In another side, IMS entities include a mass of sensitive information about subscribers' profiles, their behavior and their service use log. Securing these exchanges that contain important information has become a necessity. This paper presents our trust secure funnel based mobile service discovery and exposure model in order to define and implement security strategies to get around the problematic of malicious attacks of the available mass of information within the network and during exchanges between actors. Results shows improvement compared to other works on several axes.**

Keywords*— *IMS; Service Discovery; Service Exposure; Subscriber Profile; Funnel Approach; Security;

I. INTRODUCTION

Next generation networks are confronted to continuous evolution and improvement. The main goal is to focus on services in order to better respond and anticipate the needs and expectations of subscribers. NGN networks constitutes a subsystem that includes a diversity of services and features. This variety of services is ensured by including several actors and service providers. In another side, NGN networks contains an important mass of information about subscribers and services. Within the NGN networks architecture, it remains possible to retrieve and use information about subscribers' profiles, their behavior and their service use log. Such information may be sensitive and confidential.

Considering the important role of actors including service providers, subscribers and operators in one side, and considering the need to information exchange between these actors in another site, it remains inevitable to consider security aspects to avoid malicious attacks.

In this context, the aim of our work is to improve service discovery and exposure process by considering information exchanges that exists in the network and to include a secure strategy within these processes. Our research is based on IMS networks but may be extensible and could be applied in other fields and contexts. It should be noticed that a lot of researches and models have been developed in this field. [2] [3] [4] [8] [9] [10] [11] [14] [18] [26]

Based on previous work [19] [24] [27], we suggest to define a trust secure funnel based mobile service discovery and exposure model. We consolidate our model with different analysis to ensure its performance.

This paper is organized as follows: section 2 presents a state of the art. Section 3 develops our trust secure funnel based model and section 4 contains the conclusion.

II. STATE OF THE ART

The guideline of our work is to take advantage of information about subscribers' profiles and behaviors and to consider them in service discovery and exposure processes. Information exchange between concerned network actors within these processes is required. Thus, it will be necessary to consider security aspects all along these exchanges.

In other hand, Next Generation Networks are subject of perpetual evolution in order to guarantee adding values by well-targeted services. NGN networks presents a variety of features and a meaningful mass of information that helps getting around the discussed problematic.

Hence, in this section we will present IMS entities and components that, combined together, constitutes the information mass needed. Next, we will discuss related works that treat the presented problematic.

A. IMS related entities and features

IMS presents a subsystem that contains a relevant diversity of services to the benefit of subscribers in order to better respond to their needs and requirements. Thus, it remains interesting to take advantage of this variety of services and to consider subscribers' profiles information available within IMS subsystem in the service discovery and exposure processes to align services to subscribers' requirements.

IMS architecture is decomposed of three main layers, namely the access layer, the IMS layer (transport and control) and the application layer. Most of entities that contain information about subscribers, and services are located mainly in the control layer. The HSS (Home Subscriber Server) represents the entity that contains information about subscribers and their subscriptions to services. This entity is important to the service discovery process. The SPR

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

(Subscription Profile Repository) is an entity that treats information about subscriptions and their specificities. SLF (Subscriber Location Function) is responsible for mapping user addresses in case of many HSSs. In addition of these entities, iFC (Initial Filter Criteria) contains control logic and filters criteria to retrieve the appropriate service.

These entities, combined together, contains an important mass of information for both subscribers and services. Thus, it would be interesting to take advantage of these features to enhance service discovery and exposure processes.

Next section presents and discusses existent service discovery and exposure models.

B. Service discovery and exposure models

Several works were focused on the service discovery process [4] [8] [9] [10] [11] [14] [25] [26]. Other works considered the exposure process [2] [3] [7]. Some works treated security aspects in discovery or exposure processes [2] [3] [6] [13] [17]. Figure 1 presents an overview of approaches around these problematics.

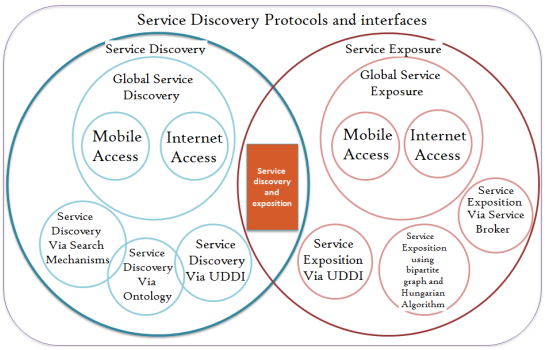

Fig. 1. Overview of service discovery and exposure approaches.

"A private, secure, and user-centric information exposure model for service discovery protocols" [2] proposes a user centric model. The idea is to expose privately and securely information within this model. Figure 2 illustrates the proposed architecture which is composed of 4 types of components, namely clients, services, directories and user agent. Processes that were considered are service discovery process and service registration process. In service registration, two steps were considered that are domain match and registration. Within this model, the service discovery process is decomposed in 5 steps that are: domain match, authentication, service selection, key distribution and invocation. Service owners or their administrators manage their domains and users utilize different roles to access services. Service owners or their administrators manage their domains. Users utilize different roles to access services. Service registration in the proposed model is selective and owner-based. A secure communication channel is established. All service accesses need to go through the directories to get permissions. This model uses a user agent to maintain all the identities of a user.

This work considers mainly security aspects in the proposed model. The service exposition process is based on services' owners. The exposure designates exposing services to be discovered by subscribers and not proposing them to subscribers dynamically. Lacks within the proposed model is response time raising because of the introduction of additional steps. Despite the consideration of security aspects, this model includes overheads and compression. Subscribers' profiles are not considered within service discovery and exposure processes. Risks of discovering services not targeted to subscribers needs remains considerable.

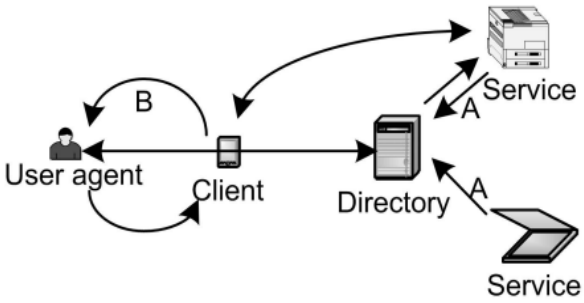

Fig. 2. Architecture components in [2].

The principle in "Expose or not? A progressive exposure approach for service discovery in pervasive computing environments" [3] is that users expose partial information about who they are and what services they are seeking. Next, if matches are found by service providers, they expose partial information about who they are and what services are available. Thus, information is exposed progressively between users and service providers until they reach a certain confidence level to authenticate for service access. If any mismatch about the service or user information are encountered during the processes, the communication stops. Advantages within this approach are the privacy and the security. This approach is also progressive and efficient and applied in a pervasive computing environment. However, it isn't a user profile centric approach. It's oriented security and treats exposure from a point of view of information and not services.

In "Secured Distributed Discovery Services in the EPCglobal Network" [6], authors present a DHT-based, scalable and secure architecture for data lookup in the EPCglobal Network. The aim is to replace the ONS (Object Naming Service) system by a secure distributed Discovery Services system. The proposed model is based on a flexible and efficient key distribution mechanism that implements the confidentiality requirement for data. The security requirements that are considered within this model are authentication, data integrity, confidentiality, availability and privacy. A level of data replication is achieved in order to ensure the robustness. This is achieved through the construction of multiple DHT-based databases using either various hash functions or the same cryptographic hash function with various keys that will be concatenated with the EPC before applying the hash function. There are no proved performances or robustness of this model which represents a considerable lack. Results stays theoretical and enhancing performances and robustness is not proven. Though, theoretically, this model enhances performances and robustness of the service discovery process and presents a secured process that fulfills security requirements. Also, this model doesn't implement a service exposure process. Besides, subscribers' profiles and behaviors are not considered in the service discovery process.

In "Private and Secure Service Discovery Using Incrementally Progressive Exposure and Random Match" [13], an incrementally progressive approach is proposed to solve the problem of subscribers' and service providers' privacy. Subscribers and service provider share a secret before interaction. Next, both subscribers and service providers expose partial encrypted information. In one side, information about subscribers' identities and service requests are partially provided. In another side, service providers share their identities and partial information about services. A step of information verification is established for both sides. If any mismatch occurs, the communication stops. Otherwise, a round of message exchange is executed until a preset number is reached. Finally, a connection is established for both

subscribers and service providers. Figure 3 illustrates the diagram of message exchange within this approach.

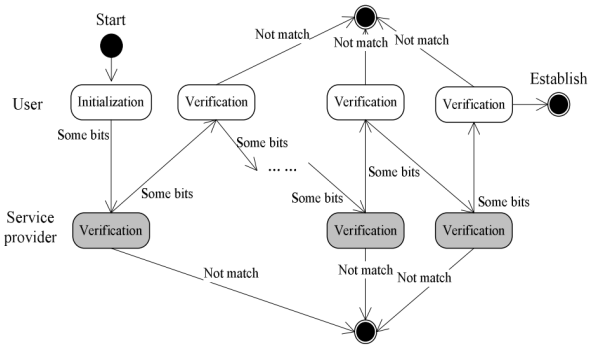

Fig. 3. The diagram of message exchange in [13].

However, through this progressive approach, the number of exchanges to reach complete match may be large. To get around this disadvantage and to reduce the number of exchanges, authors propose to increase the length of exchange message progressively. Number of sensitive information bits exchanged must stay limited in order to avoid exchanging sensitive details in case of mismatch. Figure 4 illustrates the diagram of augmenting exchange.

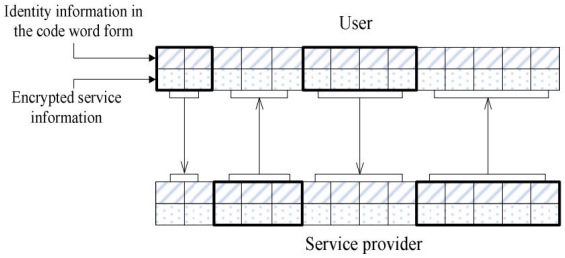

Fig. 4. The diagram of augmenting exchange in [13].

Although this incrementally progressive approach has enhanced exchanges and information privacy between subscribers and service providers, it introduces a little overhead in messages and especially sensitive information. Also, subscribers' profiles are not considered in the service discovery process. Results compared to other models may deteriorate network performances considering the number of exchanges between both sides despite the consideration of augmenting exchange.

"A trust-based dynamic secure service discovery model for pervasive computing" [17] presents a trust-based dynamic model for secure service discovery. A device which has good processing capability, network capability, and storage capacity is selected and considered as a user agent of devices within a service provider. A directory on the user agent that contains all services provided from the devices is created. The service description adopted is the following: <service name, service id, grade of service, service interface>. Next, a service classification operation in which we classify services into three levels depending on their privacy and service provider interests is implemented. A group membership test is realized based to bloom filters. A trust management unit is defined. This unit is responsible for maintaining the trust relationship between devices in order to avoid malicious users. This is ensured by calculating a value named "trust value" for all devices. Update operations for these values are established based on the service provider' or requestor' behaviors. Advantage of this model is that it considers subscribers' and service providers' behaviors in the trust evaluation. Also, results showed an improvement of response time. However, no service exposure process has been considered based on the subscriber behavior. This model may also exclude service providers that can propose more oriented services to the subscribers if they're not considered in the trust domain.

We presented and discussed in this section different models and approaches that evoke the security problematics in service discovery and exposure processes. Lacks within these models consist principally in the absence of subscribers' profiles and behaviors in the concerned processes and the overhead introduced in some models which produces performance deterioration. Service providers are not considered as proactive actors in most of the models. No service exposition operations are implemented.

In the next section, we will present and discuss our trust secure funnel based mobile service discovery and exposure model.

III. Our Trust Secure Funnel Based Mobile Service Discovery and Exposure Model

Taking into account the discussed problematic and in order to enhance subscriber experience while maintaining subscribers' and service providers' information privacy, we discuss in this section our trust secure funnel based mobile service discovery and exposure model.

We presented, in previous works [19] [27], our Funnel based JDMS-DEMO model. The guideline of this model is to consider service providers as a proactive actor. Considering available information about subscribers' profiles and behaviors, we base our service discovery process on subscribers' requirements and needs to enhance user experience. In addition to service discovery process, we set a service exposure process that is oriented to subscribers' profiles that aims to expose services to subscribers based on a provision strategy. Figure 5 represents our model overview. JDMS-DEMO considers two main actors, namely the service requestor and the service provider. Based on information extracted from several IMS entities discussed in the previous section, a matching mechanism is implemented. Based on this mechanism, service discovery and exposure processes are proposed through this model. Details about this mechanism and the proposed service broker are in [27].

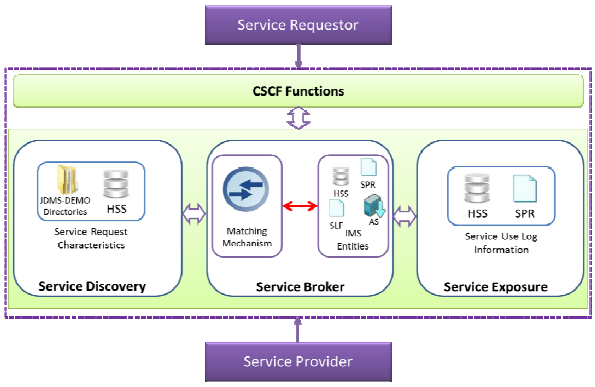

Fig. 5. Our JDMS-DEMO model overview.

We presented, in previous works [19] [27], our Funnel based JDMS-DEMO model. The idea is to consider the matching mechanism details and proceed by phases in a funnel logic. The output of this matching mechanism consists of a similarity matrix, optimized by the application of the Hungarian algorithm on it. This matrix defines the correlation between services and subscribers' profiles that are classified by

groups in directories (cf. JDMS-DEMO Directories in Figure 6) [23] [27]. Thus, the service discovery and exposure processes follows a funnel based logic that proceeds by levels based on these elements. This logic consists of a refinement mechanism in our model that contributes on enhancing service targeting and network performances. Figure 6 illustrates the discussed funnel based refinement mechanism.

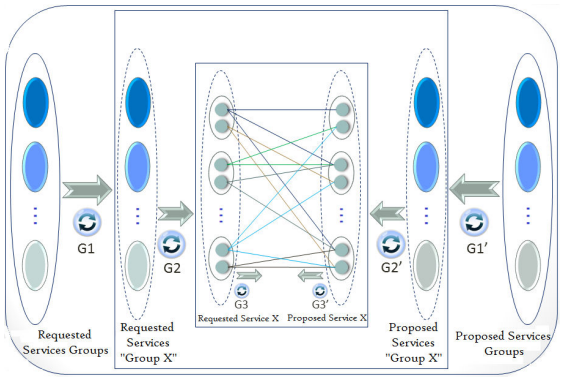

Fig. 6. Our refinement mechanism overview.

As mentioned above, within our model, beside subscribers' profiles, services are classified by groups. Thus, considering the refinement mechanism, we progress by levels in our discovery and exposure processes. At the first level, we consider the whole available services' groups. We generate then a large similarity matrix. Next, we refine our processes and we generate the new refined similarity matrix that operates on services within a specific service group. At this level, a gain in both service discovery and exposure processes is obtained (noted G1 for discovery process and G1' in exposure process in figure 7). At the second phase, the new similarity matrix generated will be refined and the same procedure is followed. A new gain noted by G2/G2' is reached. The last step of our refinement mechanism considers the requested and exposed services. At this level, a last similarity matrix is generated and a gain G3/G3' is obtained.

Within this refinement mechanism, information exchange within different steps is executed. Different subscribers or service providers may be malicious and may present risks. Thus, a strategy for a trust based secure service discovery and exposure model should be implemented. In the next section, we will present our solution to get around this problematic.

A. A trust based secure strategy

The figure 7 illustrates an overview of our model logic. Interaction between services and subscribers are mainly assured through service providers and operators. The matching mechanism presented above defines correlation between subscribers' profiles groups and services groups mainly via the similarity matrix. Also, a mass information is exchanged between both parts of our model logic. Thus, it remains necessary to secure both similarity matrix and information exchanged between operators' network and service providers' network.

Through our refinement mechanism, three steps are defined. Thus, three similarity matrixes will be generated. These matrixes define the correlation between services and subscribers' profiles. It represents the core of our model. Knowing that these matrixes are generated jointly based on information exposed by operators and service providers, a trust level between these actors should be defined. Operators should dispose of a directory that contains the list of service providers that exists in the exchange history. A trust rate should be defined within this directory.

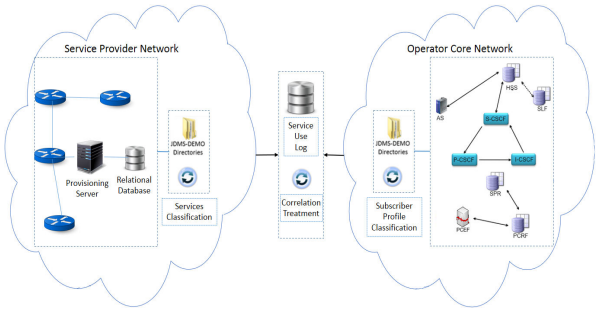

Fig. 7. Overview of our model logic.

This rate increases proportionally as exchanges with the service provider raise. The structure of this directory is presented in figure 8. It should be noticed that operators can optionally expose, totally or partially, this directory with other operators for purposes of collaborative security strategies.

JDMS-DEMO_SPT_DIRECTORY
SP_ID : [string()] <<PK>>
SP_DESC : [string()]
TrustRate: [float]
TrustLevel: [string()]

Fig. 8. Structure of « JDMS-DEMO Service Providers Trust Directory ».

With:

- SP_ID: The concerned service Provider ID,
- SP_DESC: Details about the concerned service provider,
- TrustRate: The value of the trust rate of the service provider related to the operator,
- TrustLevel: The level of trust (one of three levels) defined by the operator (detailed below).

Each operator defines two thresholds δ1 and δ2 that decompose the list of service providers into three levels of trust. Service providers that refers to the first level belong to the "high level trust zone". While dealing with them, no security constraints should be considered. They are treated as fully trusted actors. Service providers that belongs to the second level of trust should be treated with precaution. Thus, partial information should be exchanged. Sensitive information will not be exposed immediately until they reach the first trust level. At this level, the concerned operator may consult available directories of other operators and search for the concerned service provider rank. In addition, details of subscribers' profiles groups should be hidden. Exchanges with this service provider are limited only to partial similarity matrix bloc in question. The third level presents the weakest one. It regroups service providers that doesn't belong to any trust level. Treating with this level should be considered with high precaution. Information, whether sensitive or not, should not be exchanged. Exchanges with service providers of this trust level should pass upon a third part that belongs to a high trust level that guarantees both actors in each side. The decision may also be taken by the subscriber. If he certifies that the service provider is trust worthy, he can start the exchanging information process. In this case, only information about the specific subscriber are exchanged at its own risk and peril. The operator will not be responsible for any malicious operation that occurs.

We discussed, above, details about information exchange logic between operators and service providers. Next, we will discuss the information encryption in both exchange between operators and service providers and similarity matrix encryption through funnel based steps.

In our encryption, for both message exchanging and similarity matrix information, we will adopt the AES (Advanced Encryption Standard). The AES has been declared by the NIST (National Institute of Standards and Technology) as the successor of the DES (Data Encryption Standard) and has been adopted by the US government. The choice of this standard is made based on its characteristics. AES is recognized by its robustness and simplicity in implementation. It doesn't require high hardware performances to be executed and is characterized by its easiness of computation.

We presented in this section our trust secure funnel based JDMS-DEMO model. In the next section, we will present and discuss results of our experimentation.

B. *Experimentation and results*

In this section, we will discuss results of our experimentation in order to compare our trust based secure model with previous works and with other models.

Comparing our model to other models of the related work [4] and to our previous work [19] [27] is based on performances' criteria. We will discuss below results of our experimentation.

1) *Experimentation hypothesis*

In our previous experimentation [19] [27], we presented hypothesis that still significant for our problematic. Thus, we propose to keep these hypotheses in order to be comparable, namely:

- Information about subscribers' profiles and services are available,
- The data generation and structure are automated and error free,
- Getting information from directories is rather instantaneous and error free,
- The compatibility between our directories and IMS architecture is guaranteed,
- The test network configuration includes 3 virtual IMS domains (enough to be scalable to set up any session between subscribers and targeted services),
- The model and data generation follows recommendation described in [15]. This illustration of the system architecture of the considered model is shown in figure 9.

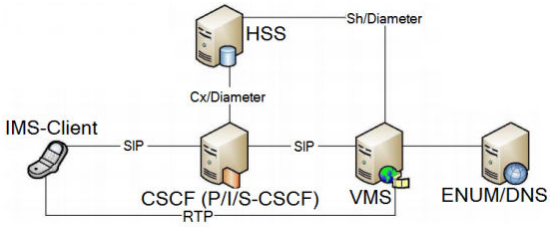

Fig. 9. IMS Test Simulator virtual domain [15].

In the next section, we will present the environment adopted in our experimentations.

2) *Experimentation Environment*

As presented in our hypotheses, our experimentation is based on 3 virtual IMS domains. Thus, the environment adopted in our context is then based on 3 virtual machines. Figure 10 presents an overview of the discussed environment.

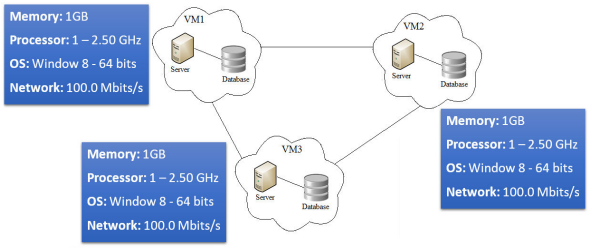

Fig. 10. Overview of the experimentation environment.

In the next section, we present experimentation results of our trust secure JDMS-DEMO model. Comparison of our model is mainly based on previous works (performant JDMS-DEMO [19]) and the OMSDA classical discovery model [4] because of the adoption of a HSS node based architecture through this model.

3) *Round-Trip Time (RTT)*

The RTT according to the number of requests shows in previous work [19] that our performant JDMS-DEMO shows an improvement compared to the OMSDA [4] model for a significant number of requests. However, compared to the performant JDMS-DEMO, our trust secure JDMS-DEMO isn't improving RTT performances. This occurs due to security strategy applied before exchanging information. The gap isn't significant and may be tolerated.

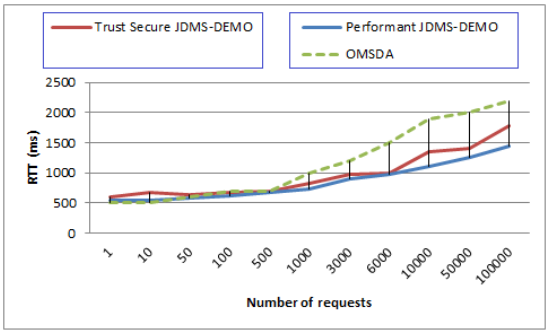

Fig. 11. Round-Trip Time (RTT) according to requests' load.

4) *CPU Utilization*

In our Performant JDMS-DEMO model [19], the CPU utilization is higher than in the OMSDA [4] classic model since it is a basic model that doesn't include advanced treatment. This gap comes from the similarity matrix generation treatment and the funnel logic application. In another side, we notice a slight increase of the CPU utilization in our trust secure JDMS-DEMO compared to our performant JDMS-DEMO [19]. This difference is explained by the processing needed to apply the AES encryption algorithm for both similarity matrix and information exchanged between actors.

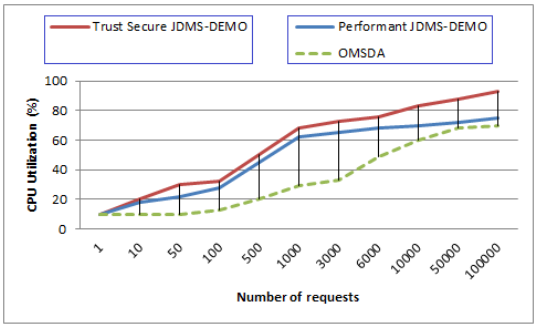

Fig. 12. CPU utilization according to the number of registered services.

5) Memory Use

In terms of memory use, results show that our Performant JDMS-DEMO [19] model presents advantages compared to the OMSDA model [4]. Considering our trust secure JDMS-DEMO, the memory use increases slightly compared to our performant JDMS-DEMO [19]. Among others, this occurs due to verification of the service provider trust level in several trust directories before starting information exchange.

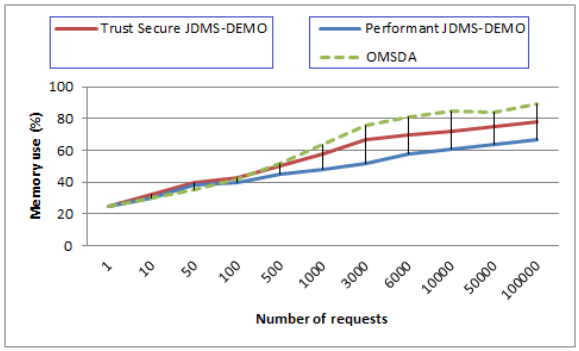

Fig. 13. Memory use according to the number of registered services.

IV. Conclusion And Perspectives

Through our secure trust funnel based mobile service discovery and exposure model, we presented a refinement mechanism applied to both discovery and exposure processes. We considered information exchange between operators and service providers. We proposed a strategy to secure information until reaching a high trust level between actors. We adopted the AES encryption algorithm that proves his robustness and that was applied in different fields.

Experimentation results show improvement of our proposed model compared to other models [4] [19] on major network performances metrics namely, round-trip time RTT, CPU utilization and memory use. A slight difference was noticed compared to previous works [19] [27] but stills acceptable.

As perspectives, our trust secure funnel based mobile service discovery and exposure model can be enriched with consideration of a conjoint decision considering preferences of the subscribers in discovery and exposure processes.

References

[1] 3GPP TS 23.228, IP Multimedia Subsystem,

[2] F. Zhu, M. W. Mutka, L. M. Ni, "A private, secure, and user-centric information exposure model for service discovery protocols", IEEE Transactions on Mobile Computing, April 2006, pp. 418 – 429,

[3] F. Zhu, W. Zhu, M. W. Mutka, Lionel Ni, "Expose or not? A progressive exposure approach for service discovery in pervasive computing environments", Pervasive Computing and Communications, 2005. PerCom 2005, 8-12 March 2005,

[4] J. ZHANG, "Optimal Model of Service Discovery Architecture Based on IMS", Young Computer Scientists, the 9th International Conference, 18-21 Nov. 2008,

[5] NIST, "Advanced Encryption Standard (AES)", National Institute of Standards and Technology (NIST), November 26, 2001,

[6] A. Dahbi, M. G. Khair, H. T. Mouftah, "Secured distributed discovery services in the EPCglobal network", IEEE International Conference on Communications (ICC), 9-13 June 2013,

[7] N. Blum, T. Magedanz, F. Schreiner, "Management of SOA based NGN service exposure, service discovery and service composition", Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium, 1-5 June 2009,

[8] H. Yu'an, W. Dongqi, Y. Tao, "Research on Service Discovery and Matching Based on Ontology and Service Capabilities in Manufacturing Grid", Computer Science and Information Engineering, 2009 WRI World Congress, March 31 2009-April 2 2009,

[9] C. A. Perryea, S. Chung, "Community-Based Service Discovery", Web Services, 2006. ICWS '06. International Conference, 18-22 Sept. 2006,

[10] N. Islam, Z. A. Shaikh, "A Novel Approach to Service Discovery in Mobile Adhoc Network", Networking and Communications Conference, 2008. INCC 2008. IEEE International, 1-3 May 2008,

[11] R. Verma, A. Srivastava, "A Novel Web Service Directory Framework for Mobile Environments", Web Services (ICWS), 2014 IEEE International Conference, June 27 2014-July 2 2014,

[12] M. Matuszewski, M. A. Garcia-Martin, "A Distributed IP Multimedia Subsystem (IMS)", World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium, 18-21 June 2007,

[13] ZY. Li, SK. Song, S. Yong, "Private and Secure Service Discovery Using Incrementally Progressive Exposure and Random Match", IEEE 10th International Conference on Computer and Information Technology (CIT), 29 June-1 July 2010,

[14] J. Zhang, "Service Discovery Architecture Base on IMS for Future NGN, Wireless Communications", Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference, 12-14 Oct. 2008,

[15] H. Zhang, "IP Multimedia Subsystem (IMS) Test Environment Simulator"

[16] W. Bethea, R. Cole, P. Harshavardhana, "Automated discovery of information services in heterogeneous distributed network", 2008. Military Communications Conference MILCOM 2008, 16-19 Nov. 2008,

[17] F. Shen, Q. Pei, S. Bu, "A Trust-based Dynamic Secure Service Discovery Model for Pervasive Computing", Seventh International Conference on Computational Intelligence and Security (CIS), 3-4 Dec. 2011,

[18] Q. He, J. Yan, Y. Yang, "A Decentralized Service Discovery Approach on Peer-to-Peer Networks", IEEE Transactions on Services Computing, Vol. 6, Issue: 1, First Quarter 2013, pp 64 - 75

[19] W. El Ayeb, Z. Choukair, "A Performant Funnel based Mobile Service Discovery and Exposure Model", The 31th IEEE International Conference on Advanced Information Networking and Applications AINA 2017, Taipei, Taiwan, March 27-29, 2017,

[20] I. Cetindil, J. Esmaelnezhad, C. Li, D. Newman, "Analysis of Instant Search Query Logs",

[21] S.A. Khanam, Kyung Hwan Oh; Woo Sik Seol, Hee Yong Youn, "A Novel Semantic Web Service Discovery Schema using bipartite graph", High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International, 13-15 Nov. 2013,

[22] W. El Ayeb, Z. Choukair, "IMS Mobile Service Discovery Search Approach", International conference on Telecommunications and ICT, ICTTelecom 2015; 16 - 17 Mai 2015,

[23] W. El Ayeb, Z. Choukair, "New Joint Dual Mobile Service Discovery Exposure Model using Bipartite Graph", The Fifth International Conference on Communications and Networking ComNet'2015, 4-7 Nov 2015,

[24] W. El Ayeb, Z. Choukair, "A Fuzzy Search Based Joint Dual Mobile Service Discovery and Exposure Model", The 30th IEEE International Conference on Advanced Information Networking and Applications AINA 2016, Le Régent Congress Centre, Crans-Montana, Switzerland, March 23-25, 2016,

[25] Y. B. Peng, Z. J. Zheng, J. Gao, X. Q. Jiang, J. Q. Ai, "Method of two stages semantic service discovery", Machine Learning and Cybernetics, 12-15 July 2009,

[26] J. Sun, X. Li, "An Analytical Model for Centralized Service Discovery Architecture in IMS Networks", Information, Computing and Telecommunication, 2009. YC-ICT '09. IEEE Youth Conference, 20-21 Sept. 2009,

[27] W. El Ayeb, Z. Choukair, "A Funnel Based Joint Dual Mobile Service Discovery and Exposure Model", 5th International Conference on Multimedia Computing and Systems ICMCS 2016, Marrakech, Morocco, September 29- October 01, 2016,

[28] J.H. Li, "Discovering Web service operations by index tables and bipartite graphs", Machine Learning and Cybernetics International Conference ICMLC, 2010, July 11-14 2010,

[29] Y. Bokhabrine, " Etude et comparaison d'algorithmes d'optimisation pour la reconstruction 3D par supershapes et R-fonctions", Laboratoire Electronique Informatique et Image UMR CNRS 5158, June, 2006,

[30] D. Hermawanto, "Genetic Algorithm for Solving Simple Mathematical Equality Problem", LIPI.