Secure and Distributed Knowledge Management in Pervasive Environments

Apostolos Malatras[1], George Pavlou[1], Petros Belsis[2], Stefanos Gritzalis[2], Christos Skourlas[3], Ioannis Chalaris[3]

[1] *Department of Electronic Engineering, Centre for Communications Systems Research, University of Surrey, UK, {a.malatras, g.pavlou}@surrey.ac.uk*

2 Department of Information and Communication Systems Engineering University of the Aegean, Karlovasi, Samos, Greece, {pbelsis, sgritz}@aegean.gr

3 Department of Informatics, Technological Education Institute, Athens, Greece, {cskourlas, ixalaris}@teiath.gr

Abstract

Pervasive environments are mostly based on the ad hoc networking paradigm and are characterized by ubiquity in both users and devices and artefacts. In these inherently unstable conditions and bearing in mind the resources limitations that are attributed to participating devices, the deployment of Knowledge Management techniques is considered complicated due to the particular requirements. This paper addresses the issue of secure and distributed knowledge management applications in pervasive environments. We present a prototype implementation after having presented detailed design principles as far as the communications and the application itself is regarded. Robustness and lightweight implementation are the cornerstones of the proposed solution.

1. Introduction

The proliferation of mobile ad hoc networking solutions observed in the past few years and the high rates of user adoption regarding this technology combined with the continuously increasing number of mobile devices [7], [8], leads us to consider that there is an established paradigm shift from traditional, infrastructure networking towards a mobile, operator – free and with no fixed infrastructure type of networking, the one based in Mobile Ad Hoc Networks (MANETs) [1]. MANET based networks together with other emerging networking technologies such as sensor networks will constitute the foundations for pervasive applications. The major strengths of this technology lie in the fact that it is easy to be deployed and has a very low cost, while allowing for user creativity through the lack of central, authoritative management [5], [6]. In the research area of mobile ad hoc networks, fundamental work was undertaken at the Terminodes project [4]. The notion of combining terminal and node capabilities in every mobile node is the driving force of this project. The notion of pervasive computing and ubiquity are strongly correlated to that of mobile ad hoc networking technologies that thus assist in reaching Weiser's innovative conceptualization of future computing [9].

MANETs undoubtedly are not a panacea for every networking problem and the emerging pervasive realm. Noteworthy drawbacks include their highly dynamic topology, since every node participating in a MANET is mobile and possibly very volatile. These constant topological variations will eventually lead to a continuous state of network instability, which in turn can extremely deteriorate the performance of applications and services on these networks. Another important issue is that typically MANET devices have limited resources as far as storage, energy and processing capabilities are concerned [2], [3]. We focus our field of networking in the ad hoc paradigm since this is the most commonly used one in the pervasive domain. It is obvious there is a need for techniques that mitigate these problems in order to be able to harness the vast range of advantages that MANETs have to offer.

Knowledge on the other hand, is probably the most important capital for an organization, constituting thus its management an issue of high significance. Modern organizations and user environments in general are characterized by a diversity and dispersion in location of both users and knowledge information, leading to pervasive scenarios like the ones described. In this paper we study the requirements needed to deploy Knowledge Management techniques in such an

0-7803-9032-6/05/$20.00 ©2005 IEEE

inherently unstable environment and propose a system architecture that enables KM operations in a distributed, robust and secure way. Main motivation for our work is the absence of significant related work. We propose a concrete solution to locate and retrieve information in an environment like the one described.

The remainder of the paper is organized as follows. After the brief introduction and motivation for our research in Section 1, related work and background literature is studied in Section 2. Section 3 analyses the requirements placed on the system design and Section 4 raises the issues related to the system's design. Section 5 describes in full the system architecture, the communication protocols amongst the entities in the pervasive domain and specific implementation details of our prototype. The paper concludes with future work and concluding remarks in Section 6.

2. Related Work

In [18] an office work scheduling tool is presented for appliance to ubiquitous environments. This system emphasizes mainly on social aspects of KM and therefore it facilitates the socialization process as defined in Nonaka's definition about organizational knowledge transformation process [19], though there is not efficient support for other KM related activities or processes. Additively, there is no direct proof about the ubiquitous characteristics of the system.

ADAM [21] is a flexible and resilient infrastructure for secure distributed knowledge exc hange, that utilises the notion of trust for authorization purposes. ADAM mainly collects knowledge related with a user's transaction history before authorizing her for transactions. ADAM handles scalability issues very effectively, though it mainly perfoms on environments characterised by total absence of well defined organizational policy. This system is not a KM system with the broader meaning of the term as it does not encompass main KM related activities.

XAROP [22] is a peer-to-peer system, which authenticates users based on the establishment of a root and subordinate PKI authorities that issue X.509 within the XAROP infrastructure. Security related knowledge asset attributes are manually defined for users and groups, raising therefore concerns about scalability potential of the non utilization of the well established RBAC authorization model.

In [10], [11] and [12] distributed service distribution on MANETs is discussed. We undertake a similar approach but we do not focus on the effects on the network performance, latency imposed, and throughput like their systems do. Our approach on distributing the lookup of knowledge sources will not deviate much but the focus will be on describing the system's efficiency in terms of the resources consumed on the device and its robustness as far as the dynamic nature of pervasive environments is considered. Network issues will be slightly ignored for now. Emphasis is being placed on providing a working and viable solution to enable knowledge management deployment on pervasive environments.

3. Requirements Analysis

The networking basis of ubiquitous and pervasive environments is that of mobile ad hoc networks. The term mobile does not necessarily mean that all the participants of the network are mobile, since any of them can be stationary for a small or large amount of time. In this environment knowledge management applications have to consider a series of issues:

- Limited resources in terms of processing power, memory capacity and energy usually characterize the devices participating in such environments. It should not be taken for granted that "thick" devices with sufficient capabilities will exist in such networks.
- Knowledge information is not limited in a closed environment as is the case in traditional networks, it spans on the contrary across multiple domains being characterized by a high degree of instability and ubiquity.
- Pervasive environments based on ad hoc networks inherit their dynamic nature. Communication links are unstable and prone on disconnections based on a variety of reasons with mobility of devices being the foremost.
- The mere notion of pervasive and ubiquitous computing adheres to the "anybody, anywhere, anytime" concept of user access to information and services around the network. This concept though incorporates a significant degree of security concerns, since especially for knowledge management systems, access to information should be controlled by access policies.

4. System Design Issues

This paper addresses the issue of knowledge management in ubiquitous environments by proposing a system that will act upon the pervasive realm and handle all the corresponding operations that need to be performed. Based on the nature of the underlying networks, which mostly follow the ad hoc paradigm, we cannot undertake the traditional approach for knowledge management systems, where – in the general case - knowledge sources would register

themselves on an appropriate service and users would query the service to gain access to the sources. Security considerations are handled by the service, by means of authenticating users to access only the knowledge information that they have clearance to do. This is the most common approach and it is push-based. Alternatively, in a pull-based approach, users may request, by flooding the network, a particular knowledge source. When a matching knowledge source identifies a request from a user, it applies security policy procedures to establish the user's validity to access its information and proceeds accordingly.

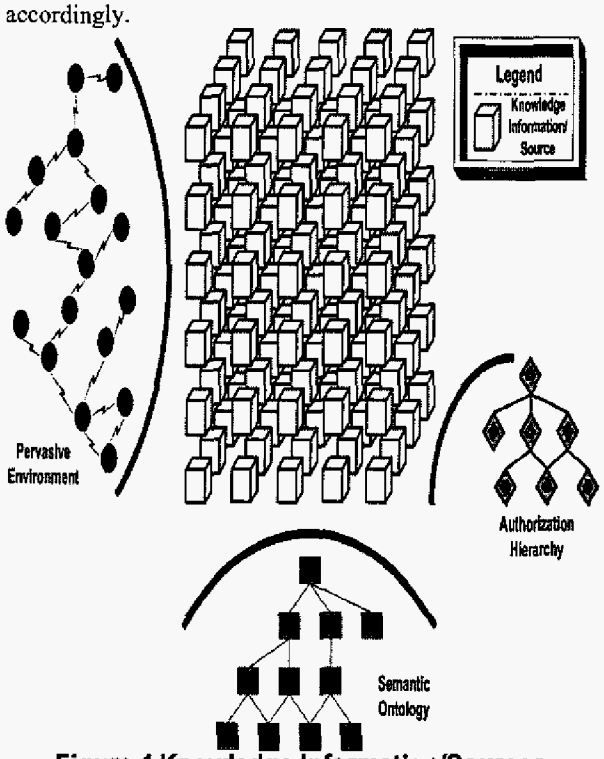

Figure 1 Knowledge Information/Sources and the aspects that characterize it

Both of these approaches cannot be considered for the unstable ad hoc environment. The former approach undertakes a centralized notion, where a lookup server is responsible for handling all the knowledge information. This single point of failure and perhaps bottleneck might be suitable for other environments, if for example one would place the server on a powerful device, but this does not stand for pervasive environments, where frequent disconnections are a norm. The system design should therefore take into account the need for robust solutions that are not dependent on the reliability of a sole device, but also consider the need to distribute the reliability perhaps through the means. The latter approach requires significant network resources to be consumed, since flooding the network with requests for knowledge sources imposes a large network overhead. Bandwidth though is a scarce resource in pervasive environments, causing this solution inapplicable in such settings.

The system we propose in this paper addresses the issues of providing knowledge management services in pervasive, ad hoc environments. Our first design principle is to distribute the management of knowledge information available in the domain amongst many devices that will collaboratively act like the lookup server did in the centralized approach. These devices will distribute amongst them the load of registering the available knowledge sources and presenting them to users upon queries placed by them. This configuration achieves the avoidance of single points of failure and lessens the consumption of resources on the devices forming the ad hoc network. This approach is considered as hybrid when the two other approaches are considered, since we have a distributed lookup server and devices do not flood the network but only part of it, until they come across a member of the distributed lookup server (DLS). Our second design principle is to enhance the searching in the ad hoc environment, since the notion of ubiquity incorporates diversity in knowledge sources and their semantic meaning. For that reason a predefined ontology is used that maps knowledge information to its terms, promoting interoperability. Security considerations form the third principle guiding our system design, with emphasis being placed on authenticating users to access the information they are allowed to. In this paper though we focus mostly on the first two principles, while the security issues constitute the basis of parallel work by our group and are not discussed further here.

Figure 1 demonstrates in a graphical way the three different aspects characterizing the knowledge information and their respective sources in a pervasive environment, as the one MANETs constitute. Borrowing from the database design and warehousing field, we can view knowledge information as information being dependent on the three axes (the aforementioned principles) of a three dimensional cube: the topology of the MANET and the corresponding location of the information, the semantic notion of the information in accordance to the existing ontology and the security clearance and authorization levels.

Of particular importance are also the protocols for the knowledge resources distribution upon a multitude of devices in the pervasive realm, namely the ones that form the DLS. There is a trade-off to consider in this case. On one hand one has to consider the special characteristics of ubiquity and act upon them by distributing the load and operations, on the other hand

though the management protocols required for this distribution should not consume the scarce bandwidth and computational resources available for the devices in typical pervasive configurations. The next section discusses in detail our proposed approach and we underline the design decisions we undertook in respect to the system design issues raised in this section.

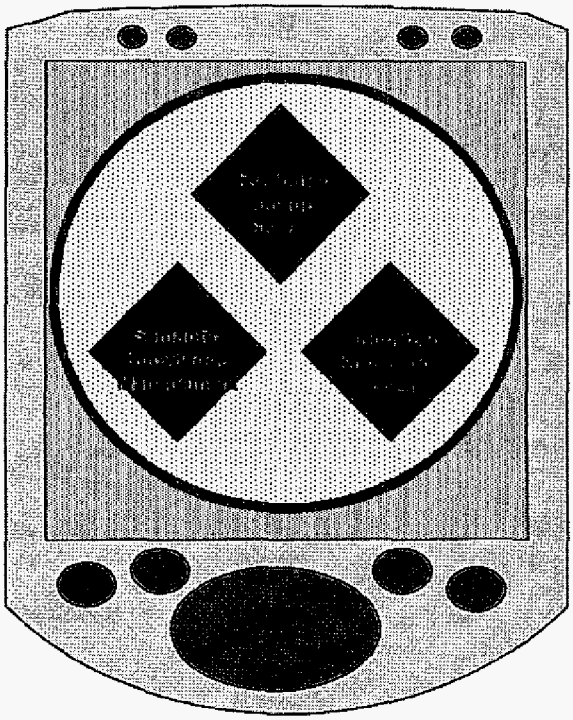

Figure 2 Components of the distributed, mobile-device oriented knowledge management system

5. System Architecture and Implementation

As we have already mentioned, the system we propose for knowledge management in ubiquitous environments is distributed and its three main parts are depicted in Figure 2. In the following sections we delve into more details regarding the system components.

5.1. Distributed Knowledge Information Lookup Server

The concept behind the knowledge information lookup server distribution is to build an overlay network on top of the ad hoc network and place upon them the distributed lookup servers. These will communicate amongst them and exchange information regarding the knowledge information they handle. Each knowledge source on the pervasive environment will register its information on one of these servers, establishing thus that all the knowledge information in the network is registered and can be reached by a member of the set of distributed servers. The idea of using a virtual backbone in the ad hoc network to be responsible for management decisions and even routing is not new. Using such a technique though for knowledge management has not been addressed though.

We can identify three basic steps to this procedure:

1. Selection of the most appropriate artifacts of the network to participate in the distributed servers set and construction and management of the set.
2. Registration of the knowledge information in the set of distributed servers and management of updates and other changes, like relocation of knowledge sources.
3. Attaching semantic meaning to the network and applying security controls to limit the access to the knowledge information scattered around the network (Sections 5.2 and 5.3).

We view that the pervasive domain can be mapped on a graph where the nodes are the devices and the links their interconnections. There have been several approaches in the literature on building distributed, collaborative management entities as virtual backbones of the graph [10], [11], [12]. The concept behind these approaches lies on the observation that centralized-management architectures are not suitable for MANETs. The need to distribute the load across the MANET is necessary for both resource constraints and reliability and robustness reasons. Solutions include connected dominating sets (CDS) of the graph, maximal independent sets (MIS) of the graph and even BFS trees. Extended work has been performed in the field and we do not wish to delve into this more, since it is not the focus of our research. In order to construct a CDS of the MANET graph we chose to discard computationally complex solutions based on approximation algorithms of the MCDS problem and solutions based on centralized approaches.

Before proceeding we have to provide some definitions in order to have a holistic understanding.

Definition 1: Every pervasive environment can be mapped on a Graph $G=(V, E)$, where V constitutes the set of artefacts comprising the environment and E is the set of links amongst these artefacts.

Definition 2: In a Graph $G=(V, E)$, a *dominating set* is a subset D of V such, that every vertex V is dominated by some vertex in D.

Definition 3: The *domination number* is the minimum size of a dominating set of G.

Definition 4: A graph $G=(V, E)$, is called *connected* when there exists a path of edges in E to connect every two vertices in V.

Freidman et al. have researched the construction of CDS in Mobile Ad Hoc networks. This is the reason we chose to adopt the connected dominating set approach and in particular the algorithm presented in [10] for the CDS construction. The details of the algorithm as adapted to the DLS context are given in Figure 3. We do not essentially differentiate ourselves from their work rather we port it to the context of knowledge information scattered in the network and knowledge management in general. The "goodness number" (used in [10]) as far as knowledge sources are concerned refers to the long-term credibility of the sources to deliver information to those who request it. This work on knowledge sources credibility is part of our ongoing research and is based on reputation schemes, we are not going to elaborate further though in this paper.

CDS Construction for Knowledge Sources in Pervasive Environments

INPUT

i: Knowledge source located on an artifact of the pervasive environment

$N(i)$: Set of i's neighbors

$DLS(i)$: Boolean value (true or false) stating the membership of i in the DLS

$Cred(i)$: Credibility value of i

OUTPUT

DLS, the set of distributed lookup servers, such that $\forall i \in DLS,\ DLS(i) = true$

RULES + ACTIONS

- $If\ DLS(i) = false \wedge \forall j \in N(i), DLS(j) = false \Rightarrow DLS(i) = true$
- $If\ \exists\ j \in N(i), (DLS(i) = true \wedge DLS(j) = true) \wedge (N(i) = N(j)) \wedge (Cred(i) \leq Cred(j)) \Rightarrow DLS(i) = false$
- $If\ \forall\ j \in N(i), (N(j) = N(i)) \wedge MAX(Cred(i)) \wedge DLS(i) = false \Rightarrow DLS(i) = true$
- $If\ \exists\ j \in N(i), (N(j) \supset N(i)) \wedge DLS(j) = DLS(i) = true \Rightarrow DLS(i) = false$

Figure 3 Construction of CDS based on [10]

When the CDS of the pervasive realm graph has been constructed the nodes that have been selected to be part of it and are consequently also members of the DLS activate the DLS service. The DLS service is installed in every artifact of the pervasive realm, but it is activated only on the members of the DLS. The next step is to register every knowledge source in the pervasive realm to the DLS, so as queries and knowledge management can take place. By definition and construction of the DLS every knowledge source will have at least one member of the DLS in its one-hop neighborhood. It is to that node that the knowledge source actually registers its existence. Figure 4 depicts an example pervasive scenario and the corresponding DLS, indicating briefly its functionality.

The Link Expiration Time (LET) amongst two nodes can be in a probabilistic way calculated. Techniques to achieve that include sophisticated solutions incorporating intrinsic measurements from GPS receivers, accelerometers and synchronized clocks, as well as probabilistic methods based on the past history movement of the nodes. In our case we adopt the LET calculation based on the transmission power samples measured from packets received from a node's neighbors [13], [14], [15]. Every node performs this action and has therefore an understanding of when a link with one of its neighbors is about to break. Members of the DLS use this information when they realize they are going to be breaking the CDS. In this case, the node that identifies the prospective link expiration issues a flood message across the network stating this situation and requesting the reconstruction of the DLS, as described earlier.

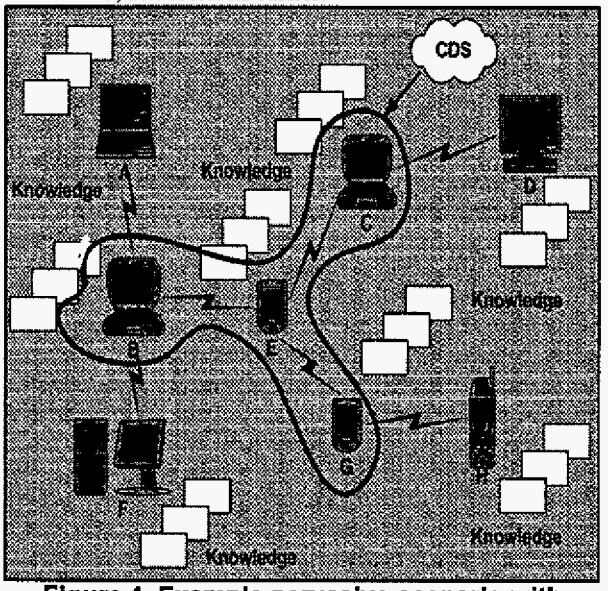

Figure 4 Example pervasive scenario with respective CDS

Obviously, this solution would not scale since it would require significant bandwidth overhead to reconstruct the DLS every time a single link breaks. We thus chose to act in two phases. If the number of link breakages predicted is larger than a particular threshold *(Max_Link_Num)* then the aforementioned procedure takes place (in the prototype implementation of our system this value is determined as 10% of the total number of nodes). When the link breakages are below the threshold value then another approach is undertaken that does involve network wide reconfigurations. The node that is about to leave finds one or more of its neighbors that collectively have the same set of neighbors and instructs them to join the DLS and activate the appropriate service. The remaining members of the DLS are also informed. Every new member of the DLS also inherits the registered knowledge sources list from the departing node.

5.2. Semantic Searching of Knowledge Information

To further enhance the knowledge management and produce more efficient results in terms of responding to users' queries on specific knowledge information we further propose maintaining a number of virtual overlay networks in respect to branches of a predefined ontology used for semantically enriching the pervasive environment. Each branch of the ontology will have knowledge information from various sources in the pervasive domain associated with it. The corresponding virtual overlay network will be built on top of the DLS and include only those artifacts that have the related knowledge information registered to them. In this way a user query will first be mapped on the ontology and then it will be flooded to a significantly smaller number of artifacts in the pervasive environment.

The user, holding a device mapped on the graph of the pervasive environment will query upon particular knowledge information. This query will be relayed to the next hop neighbor that is member of the DLS. The next step in the general case would be to flood the query among the nodes of the DLS and wait for the appropriate replies to forward back to the originating querying user. Pervasive environments can grow significantly in size, so that even the use of backbone management bodies like DLS cannot significantly assist in scaling down the increased complexity. The use of the ontology is of great significance. Major categories of the ontology are distributed between nodes of the DLS forming smaller virtual semantic sets of nodes from the nodes of the DLS. Figure 5 describes possible virtual semantic groups overlay on top of the DLS.

For example a subset can refer to information regarding e-government (Figure 5). All the relevant information sources will be registered with nodes of this overlay network and all relevant queries will be forwarded to this group of nodes. Semantic groups can be overlapping in terms of participating nodes. All nodes of the DLS are aware of the semantic groups their neighbors belong to and where to locate the nearest member of a particular semantic group. This is accomplished by referencing a specially formatted list like the one depicted in Figure 6 (coded in XML).

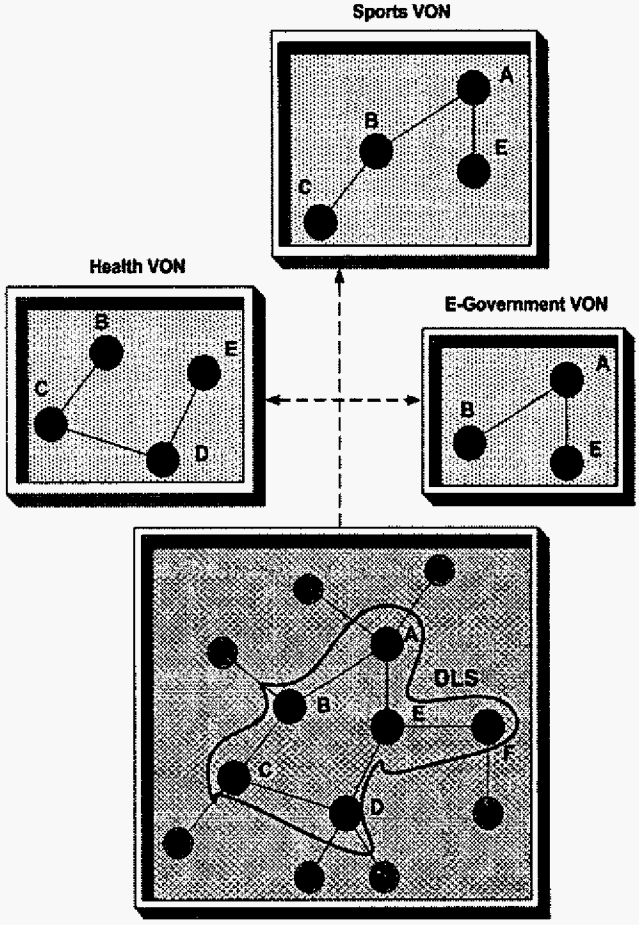

Figure 5 The DLS of the distributed knowledge environment and some indicative Virtual Overlay Networks (VON) based on the ontology semantics

To create and maintain the virtual semantic groups we exploit an approach similar to the one described for the DLS itself. Various CDS of the DLS are used to place the related service. The semantic service is an extension to the DLS service that performs the semantic categorization of queries and their mapping

on the used ontology. To avoid repetition we do no delve into much detail regarding the construction and maintenance of the semantic overlay of the pervasive environment.

5.3. Authorized knowledge information access

In order to assure authorized access the main aspects of the RBAC authorization model have been considered regarding our definition of roles and the privileges that are associated with them. Still we do differentiate from the standardized RBAC model, by not considering inheritance of properties between the roles an oversimplification which has been repeatedly questioned [23], [24]. Role inheritance as it has been proved does not reflect actual organizational structures where permission inheritance is often absent and junior roles have often different, even more permissions than junior roles. For this reason, authorization is handled through the utilization of the Extensible Access Control Markup Language (XACML), which enables context based decisions and supports role based authorizations [25]. A basic characteristic of XACML is that it enables role based policy definition as well as it supports time-restricted based activation, as defined also in the XRBAC model described in [26]. Taking into account the researched environment, we have extended the XACML authorization scheme by deploying redundant PDP and PEP entities in the network instead of only one. In our implementation we defined a set of four roles with varying authorization privileges, namely GeneralManager, DeptDirector, Manager, Employee.

Each knowledge source retains its own security policy according to its organizational structure, which leads to an assignment of different prohibitions and obligations between the different levels of security related with each role. For interoperability issues all this information is encoded in XML documents. In its full extent, the problem of dynamically establishing a negotiation of the security policies proves to be NP-complete [20]. In order to achieve a flexible and robust solution to the problem we made several assumptions. Our prototype exploits a one-to-one mapping between the organizational schemes of each knowledge source. For this reason, we implement a general scheme to which everybody needs to conform (the four roles mentioned earlier). By doing so we avoid inconsistencies between the mapping schemes on different domains and we avoid complexities while we treat scalability issues in a simple and efficient manner. We are currently working on providing more scalable anf generic solutions to this problem.

```
<pervasive_atrifacts>
    <artifact>
        <identifier>
        </identifier>
        <dls>
        </dls>
        <VON_list>
            <VON>
                <name>
                </name>
                <ontology_ref>
                </ontology_ref>
            </VON>
        </VON_list>
        <neighbor_list>
            <neighbor>
                <identifier>
                </identifier>
                <dls>
                </dls>
                <VON_list>
                    <VON>
                        <name>
                        </name>
                        <ontology_ref>
                        </ontology_ref>
                    </VON>
                </VON_list>
            </neighbor>
        </neighbor_list>
    </artifact>
</pervasive_atrifacts>
```

Figure 6 XML representation of neighbourhood information

5.4. Implementation Details

To test the proposed system's validity we proceeded in building a prototype implementation. We are also planning on testing the system's efficiency by simulation experiments; this though remains on our future agenda. We chose to first evaluate the functionality of the system in a realistic scenario and then test its scalability and dependence on various parameters by simulation, as indicated in [16].

The prototype has been implemented using the Java programming language and in particular J2ME since we are targeting mobile and pervasive environments. Being lightweight is a necessity so the CLDC (Connected Limited Device Configuration) was selected. Another reason for using Java was to grasp interoperability since in pervasive environments a variety of devices in terms of hardware/software combinations is present. The communication protocol amongst devices regarding the protocols described and the knowledge querying are implemented using the SOAP web services protocol. We understand that a

more lightweight solution like XML-RPC or even CORBA-based approaches would yield faster results, yet we chose SOAP since we want to exploit its advanced features. As we have already mentioned access and authorization rules have been built based on XACML and XML is used to keep records of neighbors and their properties (Figure 6). For the semantic ontology we used part of the Open Directory Project (dmoz.org) to serve our needs.

Each device has both the functionalities of being a simple knowledge source in the pervasive environment and of being member of the DLS. The results of the DLS construction algorithm as described earlier will indicate which of the two will be activated for each device. To be precise, the DLS members also have the simple knowledge source activated since they too host knowledge information. The memory footprint for the simple and the advanced services are minimal, requiring 21Kb and 52Kb of memory respectively. These numbers do not include the memory footprint of the J2ME platform of course.

The platform has been tested on our experimental hardware platform that consists of 10 personal computers. To be able to emulate mobile ad hoc scenarios we used the MobiEmu emulation environment [17]. We tested the platform with various mobility scenarios derived from the ns2 simulator and the initial findings prove its robustness and the ability to accurately locate and retrieve knowledge information in pervasive environments even in cases of high mobility. The links between the computers used for the pervasive scenario emulation are wireless, in particular based on 802.11b. We understand that the scenarios lack validity as far as the used devices are concerned since personal computers are more powerful from the devices that normally exist in pervasive domains; we plan to ameliorate that in the future with the use of devices with limited resources.

6. Conclusions

In this paper we presented our approach on providing secure and robust knowledge management solutions in pervasive environments based on the ad hoc networking paradigm. A prototype implementation has been built and tested on our experimental setting and the initial findings are promising, achieving adequate degrees of robustness and access to requested information. Our future work includes extensive testing of the platform in real scenarios and simulation of the DLS performance and efficiency in terms of network parameters.

Acknowledgments

This work was co-funded by 75% from E.E. and 25% from the Greek Government under the framework of the Education and Initial Vocational Training Program – Archimedes.

7. References

[1] Perkins, C. E., Ad Hoc Networking, 2001 Addison Wesley Longman Inc.

[2] Corson, S. & Macker, J., Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF RFC 2501

[3] Chakrabarti, S. & Mishra, A., *QoS Issues in Ad Hoc Wireless Networks,* IEEE Communications Magazine, pp. 142-148, February 2001

[4] Hubaux, J.-P., Gross, T., Le Boudec, J.-Y. & Vetterli, M., *Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project*, IEEE Communications Magazine, January 2001

[5] Haas, Z. H. et al., *Guest Editorial,* IEEE Journal on Selected Areas of Communication, Special Issue on Wireless Networks, Vol. 17, No. 8, August 1999, pp. 1329-32

[6] Chlamtac, I., Conti, M. & Liu, J. J.-N., *Mobile ad hoc networking: imperatives and challenges*, Ad Hoc Networks, Volume 1, Issue 1, pp. 13 –64, July 2003

[7] Giordano, S., *Mobile ad-hoc networks,* in I. Stojmenovic (Ed.), Handbook of Wireless Networks and Mobile Computing, John Wiley and Sons Ltd., New York, 2002

[8] Corson, M. S., Maker, J. P. & Cernicione, J. H., *Internet-based mobile ad hoc networking,* IEEE Internet Computing, Volume 3, Issue 4, 1999, pp. 63-70

[9] Weiser, M., *The Computer for the 21st Century,* Scientific Computer, September 1991

[10] R. Friedman, M. Gradinariu and G. Simon, "Locating cache proxies in MANETs", ACM MobiHoc 2004

[11] U. Kozat and L. Tassiulas, "Network layer support for service discovery in mobile ad hoc networks", IEEE Infocom 2003

[12] P.-J. Wan, K. M. Alzoubi and O. Frieder, "Distributed construction of connected dominating set in wireless ad hoc networks", IEEE Infocom 2002

[13] P. Agrawal, D.K. Anvekar, and B. Narendran, Optimal Prioritization of Handovers in Mobile Cellular Networks,. *Proceedings of the* R?SUT *Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication (PIMRC)*, The Hague, Netherlands, September 1994, pp. 1393-1398

[14] B. Narendran, P. Agrawal, and D.K. Anvekar, Minimizing Cellular Handover Failures Without Channel Utilization Loss,. *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, San Francisco, CA, December 1994, pp. 1679-1685

[15] Su, W., Lee, S.-J. and Gerla, M, Mobility prediction and routng in ad hoc wireless networks, International Journal of Network Management, January 2001

[16] Tschudin, C., Gunningber, P., Lundgren, H., Nordstrom, E., "Lessons from experimental MANET research", Ad Hoc Networks, Special Issue on Ad Hoc Networking for Pervasive Systems, Vol. 3, Issue 2, pp.221-233, March 2005, Elsevier, 2005

[17] Zhang, Y. and Li, W., An Integrated Environment for Testing Mobile Ad-Hoc Networks, ACM MobiHoc 2002

[18] Kida, K. Shimazu, H., Ubiquitous knowledge management - enabling an office-work scheduling tool for corporate knowledge sharing, Proceedings of IEEE Workshop on Media Networking, 2002

[19] Nonaka I., "A Dynamic Theory of Organizational Knowledge Creation", Organization Science, vol. 5, No. 1, pp. 14-37, 1994

[20] Bharadwaj V., Baras J, "Towards automated negotiation of access control policies", In proceedings of third IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'03), 2003

[21] Seleznyov A., Mohamed A., Hailes S. "ADAM: An agent-based Middleware Architecture for Distributed Access Control" Twenty-Second International Multi-Conference on Applied Informatics: Artificial Intelligence and Applications, 2004

[22] Tempich C., Ehrig M., Fluit C., Haase P., Marti E.L., Plechawski M., Staab S. "XAROP: A Midterm Report on Introducing a Decentralized Semantics based Application, Proceedings of Practical Aspects of Knowledge Management (PAKM) 2004, Vienna Austria, D. Karagiannis, U. Reimer (eds) LNAI 3336 Kluwer Academic publishers, pp. 259-270

[23] Awischus, R., Role based access control with the security administration manager (SAM), In Proceedings of the Second ACM Workshop on Role-Based Access Control (RBAC'97), pages 61–68, 1997

[24] Hitchens, M. and Varadharajan, V., Tower: A language for role based access control. In Policies for Distributed Systems and Networks, International Workshop (POLICY'01), Bristol, UK, pages 88–107, 2001

[25] XACML Oasis TC Homepage, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, accessed February 205

[26] Joshi J.B.D., Bhatti R., Bertino E., Ghafoor A., "Access Control Language for Multi-Domain Environments", IEEE Internet Computing, November/December 2004 (Vol. 8, No. 6)