A Multilevel Platform for Secure Communications in a Fleet of Mobile Phones

Serge Chaumette
LaBRI, University of Bordeaux - France
serge.chaumette@labri.fr

Jonathan Ouoba
VTT Technical Research Centre of Finland
ext-jonathan.ouoba@vtt.fi

***Abstract*—The work presented in this paper targets MANets composed of mobile phones which are possibly equipped with different wireless technologies. These nodes operate in a totally decentralized and unplanned manner by communicating with each other via peer-to-peer wireless technologies. In this particular context, the multi-technology capabilities of the mobile phones should be used efficiently to increase and diversify their peer-to-peer capacities. Therefore we have defined a dedicated multilevel platform that allows a set of mobile nodes to communicate securely in peer-to-peer mode by using the most appropriate approach depending on the context (costs and/or preferences of the entities). This paper is organized as follows. We first present the characteristics that we consider significant to build a proper model of the system. We then give an overview of the solutions that we have proposed for the main operations within our multilevel platform. Finally, we describe a mobile application that we have developed and present the performance analysis that we have conducted.**

***Keywords*-communication; peer-to-peer; wireless; mobility; security; efficiency**

I. Introduction

Current mobile devices are equipped with different wireless technologies. The combined and effective use of these technologies requires detailed analysis in terms of security and in terms of choice of the communication mean to use according to context-dependent criteria, e.g. energy consumption, financial cost. We can then synthesize the central question that we have chosen to study, in the context of the SUS[1] project, in the following manner: how to allow a set of mobile terminals to securely communicate using the most appropriate technology (in peer-to-peer mode) depending on the context? To achieve this goal, we propose to define a multilevel platform [1].
Our canonical scenario targets the sharing of information between mobile entities (or nodes). According to this scenario, we have identified the main operations to perform within the multilevel system: **the publication of a profile** which allows a node to publish the information it is willing to share with the other entities; **the specification of a set of targets** which makes it possible for a node to select the entities which may be able to provide the information it is interested in; **the choice of technology** which allows a node to select the most appropriate technology to communicate with another node of the system; **the security of communications** which is intended to prevent the unauthorized disclosure of private data.
The rest of this paper is organized as follows. We first present the target environment of the platform and our design choices. We then give an overview of the system and we describe the proposed solution. We also provide the results of the evaluations performed with an example mobile application that we have developed. Finally, we conclude.

[1]Smart Urban Spaces - http://www.smarturbanspaces.org/

II. Context

MANets are the target environment of the platform that we propose. Some of the key issues in this context are the dissemination of content, the energy preservation and the security insurance. According to existing work, we consider relevant to take into account the following aspects when modeling the platform we propose (see below): routing protocols will not be considered due to the fact that the network topology frequently changes (dynamic nature of MANets) [2], and the opportunistic approach must thus be privileged to offer solutions adapted to the environment [3]; the security of communications must be guaranteed (for example via cryptographic modules using a set of asymmetric key pairs to cipher/decipher the messages [4]); the limitation of the energy consumption is crucial, the number of messages must then be reduced as much as possible.

III. The Multilevel Platform

We believe that the level of guarantee achieved in connected networks cannot be met in MANets environments. We have consequently identified and considered the following characteristics/constraints: the effective operation of the proposed platform in a realistic environment is a priority (before considering its efficiency); the services built on top of the platform should not necessarily require 100% success of the underlying operations to be considered themselves successful (this will be discussed in section IV regarding the tests for the publication of profiles); because of brief and frequent interactions, the nodes should only exchange short text messages in a peer-to-peer mode.
In the model that we propose, each node n_i has a profile ($profile_{n_i}$). We also assume that each node embeds a Secure Element with a unique asymmetric pair of keys ($pubKey_{n_i}$ and $priKey_{n_i}$ for node n_i).

A. Publication of a profile

This operation allows a node n_i to publish its profile to the largest possible number of nodes in the network. Three cases are considered, with n_p and n_l (neighbors of n_i) being potential recipients of the profile:
case 1, transmission by relay. If n_i and n_l have a common neighbor n_m and if n_m can more easily communicate with n_l, then n_i sends its profile to n_m which retransmits it to n_l.
case 2, direct transmission. If the node n_p is an *isolated node* (it only has n_i as a neighbor), then n_i sends its profile to n_p.
case 3, default case. If a node n_l was not considered during the 2 previous steps, then n_i sends its profile to n_l.

MobiCASE 2014, November 06-07, Austin, United States

DOI 10.4108/icst.mobicase.2014.258028

B. Specification of a set of targets

This specification allows the definition of a subset of entities that a node (n_i) can target to retrieve the information it needs. n_i first establishes a set of compatible profiles ($L_{potential}$, with $N_{potential}$ being the corresponding set of nodes) via the initiation of an exploration request (within the set of received profiles, see above section III-A) making use of specific concepts of text-similarity [5]. We need additional definitions: L_{target} is the list of selected profiles with N_{target} being the corresponding set of nodes; $N^t_{n_i,isolated}$, $N_{n_i,active}$, $N_{n_i,rare}$ are respectively the sets of isolated nodes, - too - active nodes and nodes with a rare profile. Then, the following steps are considered to finalize the selection of targets:

1) $N_1 = N_{potential} \cap V_{n_i}(t)$ (we only keep the accessible nodes)
2) If $N_1 \setminus N_{n_i,active} \neq \varnothing$ then $N_2 = N_1 \setminus N_{n_i,active}$ else $N_2 = N_1$ (we try to remove the - too - active nodes)
3) If $N_2 \setminus N_{n_i,rare} \neq \varnothing$ then $N_3 = N_2 \setminus N_{n_i,rare}$ else $N_3 = N_2$ (we try to remove the nodes with a rare profile so as to use them only when absolutely necessary)
4) If $N_3 \cap N^t_{n_i,isolated} \neq \varnothing$ then $N_{target} = N_3 \cap N^t_{n_i,isolated}$ else $N_{target} = N_3$ (we try to privilege the isolated nodes because they are not otherwise solicited)

L_{target} is the set of profiles of the nodes of N_{target}.

C. Choice of technology

This operation allows a node to select the most appropriate technology (t_{choice}) to contact a given entity. First we define a cost function (for a node n_i) in a quite standard manner:

- $C_{n_i}(t_j) = \sum_{k=1}^{a}(weight_{[n_i,k]}.costMin_{[n_i,k]}(t_j)) + \sum_{l=1}^{b}(\frac{weight_{[n_i,l]}}{costMax_{[n_i,l]}(t_j)}), t_j \in techno_{n_i}$
  with $\sum_{k=1}^{a} weight_{[n_i,k]} + \sum_{l=1}^{b} weight_{[n_i,l]} = 1$
  $costMin_{[n_i,k]}$ represents the parameters to minimize; $costMax_{[n_i,l]}$ represents the parameters to maximize.

We consider two versions of the cost function, namely $C_{[n_i,e]}$ (emission mode) and $C_{[n_i,r]}$ (reception mode). We then need some additional definitions:

- $\mu_{[n_i,e]} = \min C_{[n_i,e]}$ and $\mu_{[n_q,r]} = \min C_{[n_q,r]}$
- $\tau_{[n_i,e]} = C^{-1}_{[n_i,e]}(\mu_{[n_i,e]})$ and $\tau_{[n_q,r]} = C^{-1}_{[n_q,r]}(\mu_{[n_q,r]})$
- $O_{[n_i,n_q,e]}(t_j) = (C_{[n_i,e]}(t_j) - \mu_{[n_i,e]})^2 + weight_r(C_{[n_q,r]}(t_j) - \mu_{[n_q,r]})^2$ and $O_{[n_i,n_q,r]}(t_j) = weight_e(C_{[n_i,e]}(t_j) - \mu_{[n_i,e]})^2 + (C_{[n_q,r]}(t_j) - \mu_{[n_q,r]})^2$ with $weight_r > 1$ and $weight_e > 1$
- $\theta_{[n_i,n_q,e]} = \min O_{[n_i,n_q,e]}$ and $\theta_{[n_i,n_q,r]} = \min O_{[n_i,n_q,r]}$.

Finally, the following procedure is applied by n_i:

1) if $\tau_{[n_i,e]} = \tau_{[n_q,r]}$ then $t_{choice} = \tau_{[n_i,e]} = \tau_{[n_q,r]}$
2) if $\tau_{[n_i,e]} \neq \tau_{[n_q,r]}$ then $t_{choice} = O^{-1}_{[n_i,n_q,e]}(\theta_{[n_i,n_q,e]})$ or $t_{choice} = O^{-1}_{[n_i,n_q,r]}(\theta_{[n_i,n_q,r]})$

We then use $t_{choice} = O^{-1}_{[n_i,n_q,e]}(\theta_{[n_i,n_q,e]})$ when the node n_i is seeking information from the node n_q (the reception costs for n_q are more particularly taken into account in the function $O_{[n_i,n_q,e]}$) and $t_{choice} = O^{-1}_{[n_i,n_q,r]}(\theta_{[n_i,n_q,r]})$ otherwise.

D. Security of communications

The goal is to allow a node n_i to send a message (m) to n_j in a secure manner. We use state-of-the-art mechanisms (figure 1). The transmitted packet contains information related to n_i, namely Id_{n_i} and $H(pubKey_{n_i})$. Id_{n_i} is the name n_i wants to be called by the other nodes. As for $H(pubKey_{n_i})$, it represents the hash of the public key of n_i. The packet also contains information related to n_j, namely $H(pubKey_{n_j})$, so that it can verify it is the intended recipient of the message. We use the hashes of the keys so as to have shorter messages and more efficient keys verifications. In addition, the packet includes a sequence number, $SeqNum$, to prevent an identical message from being processed several times by n_j.

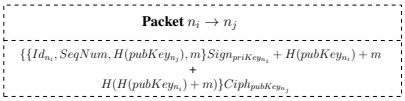

Fig. 1. Packet transmitted in secure mode between n_i and n_j.

IV. The Reference Application

We have developed an Android mobile application which is based on the specifications of our multilevel architecture. The prototype is making use of Bluetooth and Wi-Fi direct.
According to our evaluation of the energy consumption, the average overhead (induced by a one-hour use of the prototype) is about 18%. This level is reasonable as it can be put in perspective relatively to the consumption of other applications. For example the android OS built-in browser drains 0.35% of the battery for a 30s run [6]. We also verified that the method for the publication of a profile is applicable in a realistic environment. The results of our tests show that in 74% of the cases the profile is received by the nodes using Bluetooth (direct mode) and in 62% of the cases the profile is received by the nodes using Wi-Fi Direct (through retransmission). The failure percentages are to be put in perspective: we found that in 90% of the failure cases a neighbor of the node has the profile and the node can thus have access to the profile.

V. Conclusion

In this paper, we have presented the basis of an architecture to support multilevel communications within a fleet of mobile phones. First, we have proposed specifications/modelizations of the central features of the platform. Second, we have developed a prototype multilevel platform based on these specifications. We have eventually run tests that have shown that it is adapted to a realistic environment.

References

[1] S. Chaumette and J. Ouoba, "Multilevel and Secure Services in a Fleet of Mobile Phones: The Multilevel Secured Messaging Application (MuSMA)," in *Proceedings of the Fourth International Conference on Mobile Computing, Applications, and Services*, ser. MobiCASE 2012. Springer, Oct. 2012, pp. 169–185.

[2] H. Bakht, "Survey of routing protocols for mobile ad-hoc network," *International Journal of Information and Communication Technology Research*, vol. 1, no. 6, October 2011.

[3] Y. Mahéo, N. Le Sommer, P. Launay, F. Guidec, and M. Dragone, "Beyond Opportunistic Networking Protocols: a Disruption-Tolerant Application Suite for Disconnected MANETs," in *Proceedings of the 4th Extreme Conference on Communication (ExtremeCom'12)*. Zurich, Suisse: ACM, Mar. 2012, pp. 1–6.

[4] E. Atallah, P.-F. Bonnefoi, C. Burgod, and D. Sauveron, "Mobile Ad Hoc Network with Embedded Secure System," in *Ambient Intelligence Developments Conference*, Nice - Sophia-Antipolis, France, Sep. 2006.

[5] J. Ouoba, "Communications multi-niveaux sécurisées dans une flotte de terminaux mobiles (Multilevel and secure communications in a fleet of mobiles phones)," Ph.D. dissertation, University of Bordeaux, 2013.

[6] A. Pathak, Y. C. Hu, and M. Zhang, "Where is the energy spent inside my app?: fine grained energy accounting on smartphones with eprof," in *Proceedings of the 7th ACM european conference on Computer Systems*. New York, NY, USA: ACM, 2012, pp. 29–42.