PrivHab: A Multiagent Secure Georouting Protocol for Distributing Podcasts in Disconnected Areas

(Demonstration)

Adrián Sánchez-Carmona[*]
Department of Information and Communications Engineering (dEIC)
Universitat Autónoma de Barcelona (UAB)
adria.sanchez@deic.uab.cat

Sergi Robles
Department of Information and Communications Engineering (dEIC)
Universitat Autónoma de Barcelona (UAB)
sergi.robles@deic.uab.cat

Carlos Borrego
Department of Information and Communications Engineering (dEIC)
Universitat Autónoma de Barcelona (UAB)
carlos.borrego@deic.uab.cat

ABSTRACT

PrivHab is a georouting protocol that improves multiagent systems itinerary decision-making. PrivHab learns the mobility habits of the nodes of the network by building a model of the habitat of every node. Then, it uses this information to select an itinerary for each agent carrying a piece of data to reach its destination. PrivHab makes use of cryptographic techniques from secure multi-party computation to make the decisions while preserving nodes' privacy.

1. INTRODUCTION

In 2003, the Food and Agriculture Organization of the United Nations (FAO[1]) implemented a strategic Programme entitled "Bridging the Rural Digital Divide". The programme highlighted innovative approaches to knowledge exchange that were taking advantage of new digital technologies.

Thenceforth, many initiatives have been implemented in fields as e-health, e-government, e-education, e-commerce and e-agriculture. Concretely, e-agriculture applications, usually targeting rural areas, are very likely to deal with challenges due to the lack of data communication networks. It happens that regions where the communication networks are unavailable or spotty, are usually the ones where these e-agriculture services would be more needed and valuable. Unfortunately, this situation is not likely to change because the low-population density and low-income level make economically infeasible or uninteresting to extend the operators' networks into these regions.

We propose to use PrivHab to reduce the digital divide in developing countries by distributing podcast radio programs among local radio stations using Mobile Agent based Delay Tolerant Networking [2]. MADTN uses mobile agents to perform a store-carry-and-forward strategy, and it is designed to operate in scenarios where there are no simultaneous end-to-end paths. We use PrivHab to improve the itinerary decision-making of the agents carrying the data.

2. SYSTEM DESCRIPTION: THE HABITAT

The cornerstone of our novel georouting routing protocol is the **habitat**. We define the concept as the area where a node is more likely to be found.

2.1 Meaning of the habitat

The movements of every node will be strongly related to their carrier. A static node will remain immobile. A node carried by a person will probably spend much time in the vicinity of the carrier's home or workplace. A node placed in a vehicle will often pass by the same points, or it will be inside a particular area. In any case, to know the places where a node has been in the past is useful to infer if a node will visit these places again in the future. PrivHab lets the agents carrying data use this information to select the best itinerary to reach their destination. This is an assumption also made by social-based routing protocols.

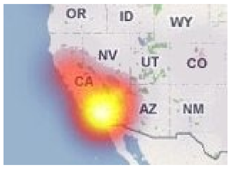


Figure 1: Heatmap of a node, the usually visited areas are depicted in dark red, and the most visited one is depicted as a intense yellow spot.

The heatmap is an extremely accurate habitat representation. However, creating and maintaining this data is a resource consuming task that does not fit with the small devices deployed by an e-agriculture application. Therefore, we propose to model each nodes' habitat using simple geometric shapes: as the circle, the ellipse or the rectangle.

2.2 Calculation of the habitat

We model an habitat using a simple geometric shape. Every node's habitat is updated periodically in order to capture the trend of the node's mobility pattern. The update process of a habitat consists in obtaining the location of a

[*] Corresponding author.

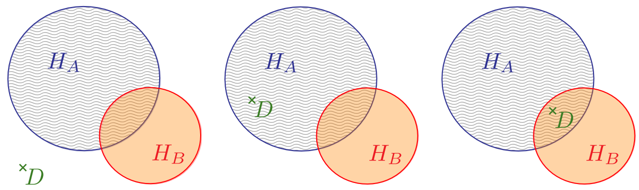
[1] http://www.e-agriculture.org/bridging-rural-digital-divide-programme-overview

Appears in: *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2015), Bordini, Elkind, Weiss, Yolum (eds.), May 4–8, 2015, Istanbul, Turkey.*

node and averaging it with his habitat's model. Location-aware nodes use the Global Positioning System (GPS) to obtain their location and the Exponentially Weighted Moving Average (EWMA) to update their previous version of the habitat with a frequency of ω updates/hour. Due to the page limit, we do not explain here the details about how to apply EWMA to each one of the shapes that can be used to model a habitat.

3. SYSTEM DESCRIPTION: PRIVHAB

The PrivHab routing algorithm compares two nodes and decides who is the best choice to carry the data towards its destination. The algorithm chooses the nodes whose habitat's border is closer to the destination, prioritizing those nodes whose habitat encloses it. If a destination is contained inside two different habitats, then the routing algorithm chooses the node with the smallest one. Figure 2 show the different situations that can be faced. In (a) and (b) node A is chosen as the best option, because the destination D is closer to H_A or inside it. In (c) the best choice is B, because both habitats contain D, but H_B is smaller than H_A.



(a) (b) (c)

Figure 2: The three possible routing situations.

3.1 A privacy-respectful protocol

At [1], the authors recognize that privacy is an important issue in a routing protocol. Nodes need PrivHab to do not reveal information about their habitats to the other parts.

Concretely, PrivHab uses the Paillier [3] cryptosystem. This cryptosystem is an additive homomorphic one, meaning that, given two encrypted operands $E(a)$ and $E(b)$, $E(a+b)$ can be computed without separately decrypting each one. PrivHab benefits from this and applies techniques of secure multi-party computation to operate the habitats and the destination and compare the results while the operands are cryptographically protected in order to avoid revealing this private information to the other parts.

4. DEMONSTRATION

In a mobile average, each time a location is used to update the habitat, previous locations lose weight. Concretely, using EWMA with using $\alpha = \frac{2}{T\omega+1}$, the last $T\omega$ locations weight the 86% of the total, while previous locations weight the remaining 14%. Figure 3 shows two examples.

The proposed demonstration contains two parts[2]. The first one is a simulation of nodes with different movement patterns. This simulation show the evolution of the habitats when the time passes and the locations are used to update them. The second one consists in an interactive software that allows the user to customize the parameters involved in the calculation of the habitat, the geometric model used, and the last $T\omega$ locations. Using this software, the user is encouraged to experiment with different configurations to see how well our habitat models a historic of visited locations.

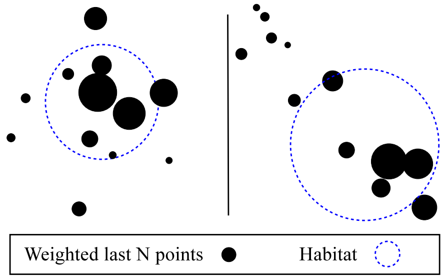


Figure 3: Examples of circular habitats (dotted) calculated with $T\omega = 12$, black bubbles depict the last 12 locations, sized according their relative weights.

5. CONCLUSION

The habitat models node's whereabouts. It is useful to compare nodes to decide who is a better choice to carry the data towards its destination. PrivHab is a secure geographical routing protocol for Mobile Agent based DTN that uses the habitats to make path-finding decisions and makes use of homomorphic cryptography to preserve nodes' privacy.

As future lines of research, we plan to improve the model of habitat using a more complex representation, and to develop an enhanced version of PrivHab that compares simultaneously three or more habitats. We also plan to study the performance of PrivHab in different scenarios based on real applications that could benefit from a geographic routing approach.

6. ACKNOWLEDGMENT

This work has been partially funded by the Ministry of Science and Innovation of Spain, under the reference project TIN2010-15764 and by the Catalan Government under the reference project 2014SGR691.

ADDITIONAL AUTHORS

Additional author: Gerard Garcia-Vandellós, Department of Information and Communications Engineering (dEIC), Universitat Autónoma de Barcelona (UAB), ggarcia@deic.uab.cat.

REFERENCES

[1] C. Boldrini, M. Conti, J. Jacopini, and A. Passarella. Hibop: a history based routing protocol for opportunistic networks. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–12, June 2007.

[2] R. Martínez, S. Castillo, S. Robles, A. Sánchez, J. Borrell, M. Cordero, A. Viguria, and N. Giuditta. Mobile-agent based delay-tolerant network architecture for non-critical aeronautical data communications. In *10th International Symposium on Distributed Computing and Artificial Intelligence*, May 2013.

[3] G. Zhong, I. Goldberg, and U. Hengartner. Louis, lester and pierre: Three protocols for location privacy. In N. Borisov and P. Golle, editors, *Privacy Enhancing Technologies*, volume 4776 of *Lecture Notes in Computer Science*, pages 62–76. 2007.

[2] See the video teaser: https://vimeo.com/116552609.