PrivHab: A Multiagent Secure Georouting Protocol for Podcast Distribution on Disconnected Areas

(Extended Abstract)

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

We consider a realistic podcast distribution application in remote rural areas, where programs have to be recorded into a CD and distributed to the local radio stations. We use a store-carry-and-forward approach, based on mobile agents, that is designed to operate in areas that lack network infrastructure. PrivHab is a georouting protocol that learns the mobility habits of the nodes of the network, then, it uses this information to select itineraries for the agents carrying the data. PrivHab makes use of secure multi-party computation techniques to preserve nodes' privacy. The PrivHab protocol is compared with a set of delay-tolerant routing algorithms and shown to outperform them.

Categories and Subject Descriptors

C.2.1 [**C.2.1 Network Architecture and Design**]: Store and forward networks; C.2.2 [**Network Protocols**]: Routing protocols, Applications

General Terms

Security

Keywords

Mobile agents; DTN routing; Applications; Privacy

1. INTRODUCTION AND MOTIVATION

In 2003, the Food and Agriculture Organization of the United Nations[1] implemented the programme "Bridging the Rural Digital Divide", highlighting innovative approaches 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. Their common goal is to universalize the access to knowledge and information to improve life condition in developing countries. E-agriculture applications, usually targeting rural areas, deal with extra challenges like a sparse population, a bad, non-existent or expensive telephony coverage, and a lack of data communication networks.

We designed PrivHab to reduce the digital divide in developing countries by distributing podcast radio programs among local radio stations or other places of interest using Mobile Agent based DTN [3]. MADTN uses mobile agents and it is designed to operate in scenarios where there are no simultaneous end-to-end paths. PrivHab improves the itinerary decision-making of the data-carrier agents by benefiting the existence of life-cycles of the users to learn about their usual whereabouts. Then, PrivHab uses this information in a secure manner to select an itinerary for each piece of data while protecting nodes' privacy.

2. SCENARIO OF APPLICATION

In some places, due to the region's dialect preference and the illiteracy ratios, radio broadcasting is the most important information source for farmers. It plays a key role in the economy development of the region by disseminating important agricultural information.

In the Cajamarca region, in Perú, the NGO *Practical Action*[2] records podcast radio programmes targeted to farmers in Compact Discs and distributes them to the local radio stations. The podcasts contain how-to explanations, newsletters, market updates, etc. This distribution method requires the NGO to spend personnel resources to bring a copy to every small local station. We aim to replace this physical distribution by a digital one by creating a Delay Tolerant Network of small devices carried by the members of the NGO's staff or by local villagers.

3. THE PRIVHAB ALGORITHM

PrivHab bases its operation in modelling each nodes' usual whereabouts using a circular habitat. This way, nodes can automatically calculate and store their habitat consuming the minimum computational resources by using an Exponentially Weighted Moving Average (EWMA), and they can use it to make routing decisions quickly.

*Corresponding author.

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

[2]http://practicalaction.org/podcasting-3

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.*

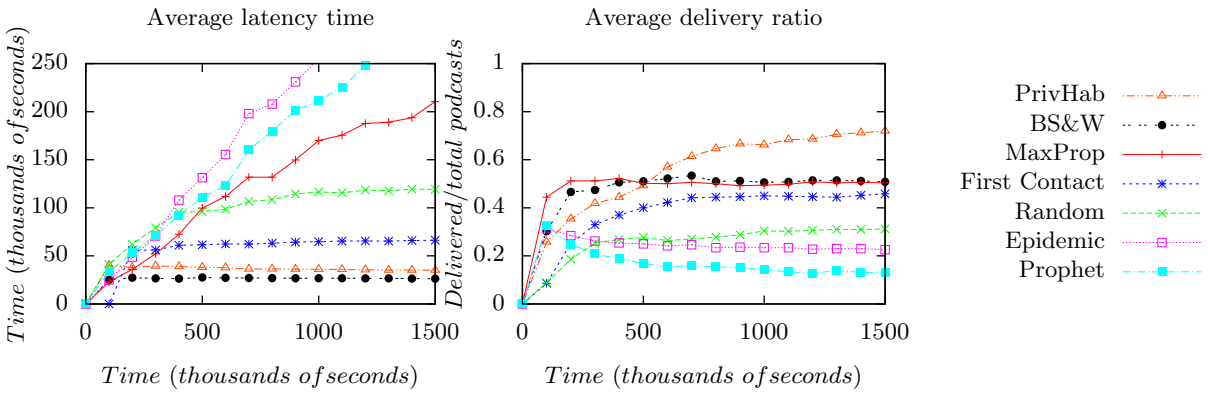

Figure 1: Latency and delivery ratio. PrivHab and BS&W perform far better than the rest.

The PrivHab routing algorithm compares two habitats and decides which node is the best to carry the data towards its destination. The algorithm chooses the nodes whose habitat's border is closer to the next waypoint (W), prioritizing those nodes whose habitat encloses it. If W 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 because the W is closer to H_A or inside it. In (c), node B is chosen because H_B is smaller than H_A.

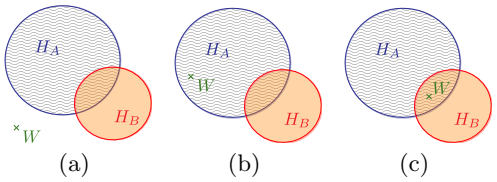

Figure 2: (a) The waypoint is located outside the two habitats; (b) Only one of the habitats encloses the location of the waypoint; (c) The two habitats enclose the location of the waypoint.

Habitats are used during itinerary selection, but they can not be made public, since this will hurt the privacy of nodes. For this reason, PrivHab requires an additive homomorphic cryptosystem. An additive homomorphic cryptosystem is one in which, given two encrypted operands $E(a)$ and $E(b)$, $E(a+b)$ can be computed without decrypting each one. The cryptosystem used by PrivHab is the Paillier [4].

PrivHab makes use of this property to compare two habitats, following the routing algorithm described above, without disclosing any habitat's information.

4. EXPERIMENTS AND RESULTS

We have deployed a proof-of-concept implementation of PrivHab on three Raspberry Pi boards. These are very cheap low-end devices that fit with the characteristics of the described scenario. We have used them to measure the PrivHab's overhead that PrivHab. The obtained execution time, using keys of 1024 bits[3], is 3.9 seconds. Given the average length of connectivity windows in remote village scenarios [1], this overhead is acceptable.

Besides, we have compared the performance of PrivHab with a bench-mark of routing protocols: Prophet, BS&W (L=40), Epidemic, Random, MaxProp and First Contact, using *The Opportunistic Network Simulator* (The ONE) [2].

As it can be seen in Figure 1, PrivHab delivers more data to its destination, and it does it faster than other protocols except BS&W. Moreover, it preserves nodes' privacy. We can state that PrivHab is the protocol that suits better to any scenario with characteristics like the presented one.

[3]The effort needed to break the provided security is equivalent to the effort needed to factor a 1024 bits RSA key.

5. CONCLUSIONS

In this paper, we have presented PrivHab, a secure geographical routing protocol for Mobile Agent based DTN that uses the habitats to make routing decisions and homomorphic cryptography to preserve nodes' privacy. We have presented a podcasts distribution application in rural areas that benefits from its characteristics and performance.

6. ACKNOWLEDGMENT

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

REFERENCES

[1] S. Grasic and A. Lindgren. Revisiting a remote village scenario and its dtn routing objective. *Computer Communications*, 48:133–140, 2014.

[2] A. Keränen, J. Ott, and T. Kärkkäinen. The ONE Simulator for DTN Protocol Evaluation. In *SIMUTools '09: Proceedings of the 2nd Int. Conf. on Simulation Tools and Techniques*, 2009.

[3] 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 Springer, editor, *In 10th International Symposium on Distributed Computing and A.I.*, May 2013.

[4] 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.