Secure Channel Service for MANETs

Francesco de Angelis, Jose Luis Fernandez-Marquez and Giovanna Di Marzo Serugendo
University of Geneva, ISS, Battelle, Batiment A, Route de Drize 7, CH-1227
Carouge SWITZERLAND
{francesco.deangelis, joseluis.fernandez, giovanna.dimarzo}@unige.ch

I. Introduction

Mobile Ad-Hoc NETworks (MANETs), composed of mobile phones, tablets, or laptops provide huge infrastructures that connect wirelessly people, cars and public devices (e.g. traffic lights or public displays) without relying on the Internet or mobile phone operators. These infrastructures open opportunities for the development of a wide range of innovative applications, such as crowd steering (e.g. Emergency evacuation of a building or an area, or tourist guides), context-aware navigation (e.g. finding a place, finding a person in a crowded area), or rescue (e.g. survivor localization or communication between emergence services).

In most of these applications, privacy and routing play a key role and their combination represents an important field of research in the context of security for MANETs ([1]). The node mobility and the wireless transmission of data make it susceptible to eavesdropping, while dynamic routing is essential to maintain a communication channel between two mobile entities.

Currently MANETs applications, as well as self-organizing applications in general, are being designed and prototyped in an ad-hoc manner without reusing functionalities.

The main contribution of this paper is to show how to use a well defined set of self-organizing services [2] for establishing and preserving a confidential and adaptive channel between two communicating entities in such a mobile networks. Building applications on top of self-organizing services turns to be an effective technique for reducing the effort of the development of self-* applications by promoting code reusability and robustness.

II. Self-organizing Services

Such a self-organizing services provide a layer of abstraction favoring separation of activities: applications are developed by delegating to underlying self-organizing services all communication issues and difficulties related to the dynamics of the environment, i.e. mobility, disconnections, or access of new nodes.

The computational environment is a key entity and it provides reliable "CORE" services [2], i.e. low-level self-organizing mechanisms (e.g., gradient, digital pheromone), and proposes them to the applications under the form of ready-to-use "operators" or "services". The implementation of higher-level self-organizing services and applications is achieved in a modular way, reusing mechanisms, decoupling them from the application functionality and delegating responsibilities for them to the computational environment.

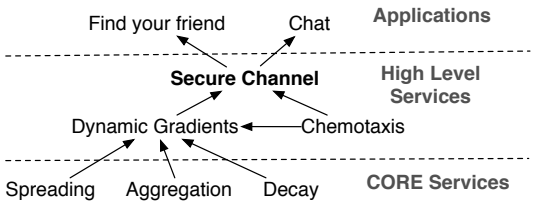


Fig. 1: Secure Channel Service Composition

Figure 1 shows the self-organizing services used to build the Secure Channel Service. Namely, they are:

Spreading is a service that propagates information among the nodes of the network.

Aggregation service allows the system to reduce the amount of information spread in the system or taken from the environment.

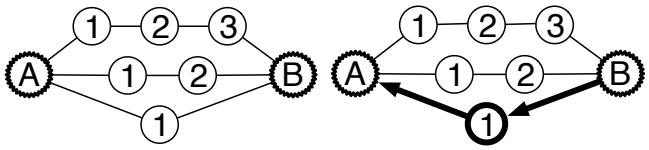
Decay service, also called evaporation service, helps dealing with dynamic environment. It decreases periodically the information relevance, in order to get rid of outdated information.

Dynamic Gradients service combines the Spreading, Aggregation and Evaporation services in order to provide a spatial structure that contains information about the sender's (source) distance (i.e. hops number) and direction. The gradient is progressively propagated among nodes, aggregated by keeping the information with the minimum hop counter, and evaporates with time.

Chemotaxis service allows information to be routed to the gradient source by following the gradient information.

III. Secure Channel Service

The Secure Channel service provides an encrypted channel for routing confidential communication between devices in a mobile ad-hoc network. The computational power and memory available in mobile devices are increasing dramatically, allowing now the use of traditional encrypting techniques that some years ago were available only in wired computers, such as laptops or PCs. Therefore, the Secure Channel service uses RSA encryption on top of Dynamic Gradient and Chemotaxis services in order to ensure and maintain confidential communications and routing even in complex mobile networks. Such a definition provides a new way for establishing and keeping the secure channel updated without requiring additional tasks from the application developer's point of view.



(a) Gradient Creation (b) Encrypted Information routed

Fig. 2: Secure Channel Service phases

Let be A and B two nodes in a MANET. A wants to receive some private information from B. The different phases of the Secure Channel service are the following:

- Using a Gradient service, node A sends a public key and a request for information. They are both propagated to all nodes in the network along with additional gradient information about the sender's distance (e.g. number of hops).
- When the Gradient reaches node B, the latter retrieves the query and the public key. B encrypts the information using the received public key and sends it back along the shortest available path by using the Chemotaxis service.
- The gradient structure is updated periodically in order to deal with network topology changes. This activity is performed automatically by the combination of Dynamic gradient and Chemotaxis services.

We assume the identity of a user is stated by means of an authentication protocol.

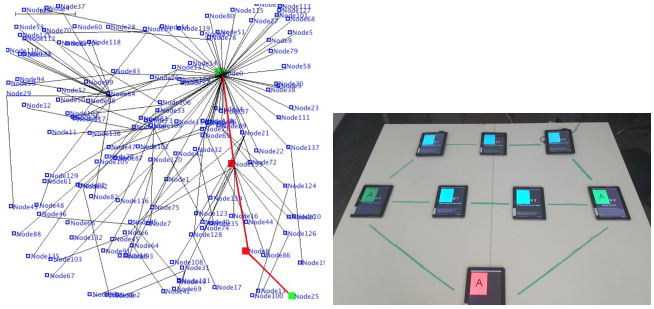
IV. Implementation and validation

The Secure Channel Service has been developed by using the SAPERE middleware [3], [4], which combines chemical reactions, active tuple spaces, rule-based systems and self-organizing design patterns in order to provide a middleware that allows the design and implementation of pervasive and self-organizing applications in a modular way.

We highlight here two aspects of the development and deployment of the Secure Channel Service: (1) the prototyping phase using a simulator and (2) the deployment on real devices.

To alleviate the difficulty of debugging and producing useful tests in MANETs we undertook a prototyping phase by using a version of The ONE simulator extended with the actual SAPERE middleware. During the simulation each node executes an instance of the middleware and delegates to the simulator the management of nodes mobility, communications and collisions. The assessment of the Secure Channel Service has been realized by validating several different scenarios with The ONE simulator, before proceeding to its deployment on real Samsung tablets connected locally by a logical network.

Figure 3(a) shows a screenshot of the simulation with 150 nodes. Node 0 requests a private information to node 25. The red path is the one used to route the encrypted information and it evolves dynamically as nodes move. Figure 3(b) shows a picture of the implementation using Samsung tablets.



(a) Simulation (b) Real devices

Fig. 3: Secure Channel Service Implementation

Implementation details regarding the simulation and the deployment on real devices are provided in http://www.cui.unige.ch/~deangeli/SasoDemo2013.mp4.

V. Conclusions and future work

This paper discusses the engineering of a Secure Channel Service for providing confidentiality in Mobile Ad-hoc NETworks by using self-organizing services; the service has been assessed with The ONE simulator and it is provided as a SAPERE middleware library for Android devices. The authentication functionality, intentionally neglected here along with the key-management activity, can be provided by several well known algorithms, as reported in [5] and [6].

We intend to extend this work into a Secure Multi-Channel service, allowing the routing of encrypted information using many different channels at the same time. Further works could focus on the security of the routing protocol itself in addition to confidentiality, facing the well known attacks reported for instance in [7].

Acknowledgment

This work has been supported by the EU-FP7-FET Proactive project SAPERE Self-aware Pervasive Service Ecosystems, under contract no.256873.

References

[1] T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in MANET routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 9, pp. 70–84, 2007.

[2] J. L. Fernandez-Marquez, G. Di Marzo Serugendo, and S. Montagna, "Bio-core: Bio-inspired self-organising mechanisms core," in *Bio-Inspired Models of Networks, Information, and Computing Systems*, ser. LNCS, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, 2012, vol. 103, pp. 59–72.

[3] F. Zambonelli et al., "Self-aware pervasive service ecosystems," *Procedia Computer Science*, vol. 7, pp. 197–199, Dec. 2011, proc. of the 2nd European Future Technologies Conference and Exhibition 2011 (FET 11).

[4] F. Zambonelli, G. Castelli, M. Mamei, and A. Rosi, "Integrating pervasive middleware with social networks in SAPERE," in *Int. Conf. on Selected Topics in Mobile and Wireless Networking*, 2011.

[5] J. V. D. Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Comput. Surv.*, vol. 39, no. 1, Apr. 2007. [Online]. Available: http://doi.acm.org/10.1145/1216370.1216371

[6] S. Boonkrong and R. Bradford, "Authentication in mobile ad hoc networks."

[7] W. Li and A. Joshi, "Security issues in mobile ad hoc networks - a survey."