Security Issues in Opportunistic Networks

[Extended Abstract]

Abdullatif Shikfa
EURECOM
2229, route des Crêtes - BP 193
06560 Sophia-Antipolis, France
shikfa@eurecom.fr

ABSTRACT

In this extended abstract we present a work on security issues in opportunistic network that were studied in the framework of a PhD program. In particular we analyze the problems of cooperation enforcement and of secure context or content based routing and propose suitable solutions.

Categories and Subject Descriptors

C.2.2 [**Computer-Communication Networks**]: Network Protocols

General Terms

Security

1. INTRODUCTION

Mobile Opportunistic Networks (MobiOpps) are an extreme generalization of Mobile Ad-Hoc Networks (MANETs), that aim at enabling communication between mobile nodes in highly challenged conditions, which raise new networking and security issues due to:

- Heterogeneity: as in MANETs, nodes cannot rely on a global infrastructure and on top of that they belong to heterogeneous networks that rely on various communication technologies. This means in particular that naming is an issue, because nodes don't have a unique address across the different networks and furthermore raises the requirement for new authentication and trust establishment mechanisms.
- High mobility: nodes are extremely mobile and disruptions in paths are frequent. It is thus impossible to establish a stable end-to-end route: routing and security solutions should be highly dynamic and flexible, and should not depend on a pre-defined path.
- Delay tolerance: since nodes belong to heterogeneous networks, an end-to-end path might simply never exist. Messages can still be delivered by adopting a store and forward strategy, where intermediate nodes store messages when communication is impossible and forward them when a communication opportunity arises, for example thanks to mobility. Such a strategy trades a higher delay for a higher delivery ratio, but this also means, from a security point of view, that direct interactions cannot be assumed: end-to-end key agreements are thus unpractical and all protocols relying on an on-line authority need to be revisited.

Because of these characteristics, MobiOpps call for a radical revision of all security aspects of communication, and in the following we present an overview of our work on cooperation enforcement and secure routing in MobiOpps.

2. COOPERATION ENFORCEMENT

In MobiOpps, there is no infrastructure and in particular no designated routers: all nodes are expected to take part in the forwarding process in order to increase the communication opportunities and the throughput along. This raises the issue of selfishness: nodes are inclined to forward only packets that interest them while ignoring others. This issue is even more critical for small devices as scarcity of resources fosters selfish behavior. Nodes need therefore incentives in order to cooperate with each other for the greater good.

This issue has already been studied for MANETs but the solutions proposed cannot apply to MobiOpps. Indeed, currency-based cooperation enforcement schemes rely either on costly tamper-proof hardware [2] or on an online trusted third party [7] which is not compatible with the delay tolerance characteristic, while reputation mechanisms like [3] require stable network configuration and a large amount of time to establish trust.

We therefore proposed in [4] a new approach to enforce cooperation that fits MobiOpps requirements. This solution is based on the hot potato approach where nodes have to take a decision of accepting to receive a packet and paying for it or not blindly. If the node then discovers that the packet is not interesting for him, it is incited to forward the packet to other nodes in order to get its payment back, hence cooperation is enforced. This protocol achieves optimistic fair exchange: if a conflict occurs an authority guarantees fairness by giving each party its rightful part, but the authority is not required in case of correct execution of the protocol. This protocol sketch shows that this approach is suitable for MobiOpps because it does neither require prior trust establishment nor online authority and it is flexible: nodes can decide not to receive packets (e.g. if their resources are low), but in this case they might miss packets destined to them, or they can decide to collaborate with others to receive packets destined to them and forward other packets.

MobiOpp '10, February 22-23, 2010, Pisa, Italy.

3. SECURE ROUTING

Routing in MobiOpps is a compelling issue: in the absence of a global infrastructure, addresses are network-specific and have no meaning outside, hence naming becomes an obstacle. Thus conversational communication between a source and a destination is replaced by content dissemination where destination are implicitly defined by their interests or their context rather than an explicit address.

In context-based forwarding the destination is implicitly known through its context while in content-based forwarding the source does not know anything about the destination: the destination has to express its interest which are not intrinsically linked to a particular node. Both these approaches present challenging privacy issues because context and content are private data that need to remain confidential but intermediate nodes still need to access the context or content to perform networking operation. These conflicting requirements between routing and privacy call for innovative solutions and we present an approach for each case.

3.1 Privacy-preserving context-based forwarding

In context-based forwarding the destination is not directly known by the source, but the source knows context attributes of the destination. The destination's context is a private information that should be protected and not be sent in the network cloud. A natural idea is therefore to use identity-based encryption by replacing the identity of the destination by its context attributes. This solution manages to create an end-to-end secure channel between source and destination but it prevents context-based forwarding. Indeed in context based-forwarding, intermediate nodes need to compare their context with the destination's context. Each intermediate node should therefore be able to discover the matching attributes with the destination while not learning any additional information on other attributes to preserve destination's privacy.

This is reminiscent of the general problem of searchable encryption, and we propose in [6] a solution based on Public Encryption with Keyword Search (PEKS) [1] to enable intermediate nodes to search for matching context (the keywords). There is yet an additional difficulty: in PEKS, the destination is known and gives intermediate node the capability to search for a given keyword thanks to trapdoors, while in context-based forwarding the destination cannot give trapdoors to all intermediate nodes because of the challenging environment and the destination is unknown anyway. We address this issue by modifying the mode of operation of PEKS to fit our requirements: we replace the destination by a trusted third party (TTP) that is in charge of providing each intermediate nodes with trapdoors corresponding to their context. The TTP need only to be contacted once before nodes join the network and is offline during the network operation, which is suitable for opportunistic networks. Furthermore this solution allows intermediate nodes to compute the matching ratio between their context and the destination's context and to forward the message to nodes that show increasing match, thus enabling privacy preserving context-based forwarding.

3.2 Secure content-based routing

In content-based communication there is a complete decoupling between sender and receiver: intermediate nodes build their routing tables based on the interests advertised by receivers. These interests are private information and it is therefore important to guarantee the confidentiality of advertisements while still enabling intermediate nodes to build their routing tables. This issue is very different from the previous one because contrary to context, interests are not intrinsically linked to a node and they change frequently. The problem is therefore to enable intermediate nodes to build routing tables with encrypted interests and to perform secure look-up of encrypted content in the routing tables.

To achieve this goal, we propose in [5] a solution based on multiple layer commutative encryption (MLCE). The idea is for a receiver to encrypt its receiver advertisement with r layers corresponding to the r next hops using r different keys, and for the publishers to do the same with their published content. An intermediate node N en-route can remove only one encryption layer so that the data is always protected by at least $r-1$ layers of encryption. Thus N does not have access to data in cleartext, but it performs the setup of routing tables and takes forwarding decisions on data encrypted $r-1$ times. Then N adds a new encryption layer corresponding to the r^{th} next hop without destroying the other layers thanks to the commutativity of the cryptosystem and transmits the message.

By rotating the encryption layers, this solution enables content-based routing that preserves privacy of receivers very efficiently in a decentralized way. Furthermore, despite the lack of end-to-end connectivity, end-to-end confidentiality is still achieved with a local key agreement protocol.

Acknowledgments

This work has kindly been supervised by Prof. Refik Molva and Dr. Melek Önen and has been supported by the European Commission projects HAGGLE and SOCIALNETS.

4. REFERENCES

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In *EUROCRYPT*, pages 506–522, 2004.

[2] L. Buttyan and J. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks*, 8(5), October 2003.

[3] P. Michiardi and R. Molva. Core: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. In *IFIP Communication and Multimedia Security Conference (CMS)*, 2002.

[4] M. Önen, A. Shikfa, and R. Molva. Optimistic fair exchange for secure forwarding. In *SPEUCS 2007, 1st Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems, August 10, 2007 - Philadelphia, USA*, 08 2007.

[5] A. Shikfa, M. Önen, and R. Molva. Privacy in content-based opportunistic networks. In *WON 2009, 2nd IEEE International Workshop on Opportunistic Networking, May 29, 2009, Bradford, UK*, 05 2009.

[6] A. Shikfa, M. Önen, and R. Molva. Privacy in context-based and epidemic forwarding. In *AOC 2009. 3rd IEEE International WoWMoM Workshop on Autonomic and Opportunistic Communications, June 15, 2009, Kos, Greece*, June 2009.

[7] S. Zhong, J. Chen, and Y. Yang. Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. In *Proceedings of Infocom*, 2003.