On Opportunistic Networking Security

Bernhard Distl, Franck Legendre
CSG – ETH Zurich, Switzerland
last_name@tik.ee.ethz.ch

1. INTRODUCTION

With the advance of mobile devices, a variety of new networking scenarios and applications are emerging. One challenging kind of networking paradigm are opportunistic networks. Opportunistic networks are formed by mobile users carrying their devices, that take advantage of any wireless contact opportunity. This networks are decentralized and assume no access to any fixed infrastructure and central authority (e.g. PKI). Possible operational areas are remote and rural areas, urban public domain networks and emergency situations with applications ranging from content distribution to social networking. In this paper, we survey existing networking paradigms (wired, Ad-Hoc, DTN) and put them into relation with opportunistic networks, pointing out differences and similarities among them. Because of these differences, opportunistic networks face challenging security issues. We highlight threats and proposed solutions and then emphasize current security approaches that are suited for opportunistic networks. Eventually, we call for a new approach for security in opportunistic networks.

2. ATTACK THREATS

While in classical networking as well as P2P and Ad-Hoc networks we see connected networks (space paths), for DTN and opportunistic networks the connection is also established over time (space-time paths). This is also reflected in the security assumptions, where classical networks use centralized and P2P and Ad-Hoc use decentralized structures both assuming connectivity. For opportunistic networks and DTNs disconnected decentralized approaches are necessary. Regarding dynamics we see node arrivals/departures as churn in P2P networks which is similar to inter-contact times in opportunistic and DTN networks. In contrast to Peer-to-Peer and Ad-Hoc networks, where a structure is artificially imposed, opportunistic networks exhibit a structure based on the social network the device users are part of. This given structure in turn can be used to create new security mechanisms [8].

All of the networking paradigms face possible attacks where some of them are generic while others are specific to certain network types. Generic attacks divide into loss of confidentiality, integrity (e.g. manipulation), availability (e.g. DoS) or authentication (e.g. impersonation [2]).

Routing. Specific to routing there are threats like black hole or wormholes or traffic diversion. Some routing schemes are subject to a wider variety of attacks than simple routing schemes like flooding. Some services, like opportunistic content distribution, can even be based on user solicitation (user driven download), thus avoiding routing and its related security issues.

Application attacks. One prevailing application attack is spam, which is not only possible in the wired network email system, but also in Web 2.0 applications like Facebook and can also be implemented in opportunistic content distribution.

PodNet [5] is an application and testbed which allows exchanging content in an opportunistic way between mobile devices using ad hoc radio communications. The PodNet project targets the mobile content distribution by extending the traditional podcasting concept for public (i.e. open and unrestricted) peer-to-peer content delivery among users. While we have already been successfully able to demonstrate it working, security issues are not yet fully understood.

3. SURVEY OF SECURITY APPROACHES

An often used classical approach to solve security issues in wired networks is done in a centralized way using a PKI, which can often not be used in other forms of networking where either a centralized structure can not be built, or the connectivity to central components can not be maintained all the time. Another reason not to use a centralized security solution is, when many parties are involved that can not agree on a common infrastructure.

Technologies used in Peer-to-Peer and Ad-Hoc networks, like threshold cryptography or solutions based on DHTs typically assume, that a specific node (group) in the network can be reached at any given time. Those solutions allow for decentralized storage and manage-

ment of the security mechanisms as well as distributed computation of security measures, but still rely on the timely retrieval of information from the network [4].

It seems as there is not much work on security in DTN available. Some security aspects are treated e.g. in [7] and [1]. Since opportunistic networks are not yet a common research topic, there are no security mechanisms designed specifically for them. Some mechanisms that are proposed for Ad-Hoc and P2P networks could be applied in an opportunistic context, where we see characteristics of Ad-Hoc networks as well as from DTNs.

An opportunistic content distribution system like PodNet, while it avoids routing in the classical sense, faces a lot of security challenges. In a recent extension we investigated experimental spam control mechanisms. Mitigating sybill attacks in a distributed way is one of the most challenging tasks [9].

4. CURRENT WORK

As this PhD work is in an early stage, this presents only an outline and direction of intended work and no actual results.

Topic definition. We will work in the field of opportunistic networking, specifically looking at security strategies. The mechanisms might fit for DTNs as well as opportunistic networks. Evaluation of security designs will be done in the context of opportunistic content distribution and possibly by experimentation in our PodNet testbed. Possible approaches are outlined in the following paragraphs.

Inherent Characteristics. As connectivity is only available among devices that are in mutual transmission range, any centralized security solution will not be available when needed and by the large heterogeneity among all users, it is unlikely, that it is possible to agree on one central "trusted" instance for all. There are characteristics that can be exploited. Since participating devices are carried by users, the mobility of the user can be used to derive information about contact patterns and properties. This can in turn be used for link prediction or environment detection. Users interactions will also show patterns that refer to their position and ties in their social network. Social networks themselves are a popular research topic and we believe, that this inherent social network aspects will not only drive new applications but also new security mechanisms. Friends are one important role in social networks, that can be used to construct security mechanisms. Those security relationships will be based on trust links within the social network.

Enforcing Mechanisms. Based on inherent characteristics and additional mechanisms it is possible to increase the security in opportunistic networks. One example is rating of transactions or received content by the recipient. By evaluating the ratings and optionally exchanging them among users, additional improvements can be made to security. There are many rating systems available, some of them potentially suited for the opportunistic case [6]. Community Detection [3] is another way of deriving potentially useful information from the contact patterns and the social network. While community detection at the moment seems a difficult task, some basic concepts are already available. Their reliability for opportunistic networking has yet to be determined. We have developed a first draft of a security framework for opportunistic content distribution that was implemented within our PodNet testbed.

Our Approach. We intend to first evaluate relevant existing approaches with regard to their use in opportunistic networking. For opportunistic content distribution we have proposed a security mechanism that is able to attribute specific content to a certain author, prevents others from claiming another authors identity (SUCV [2]), provides content integrity, and allows for rating. The introduction of a rating scheme that additionally enhances the quality of the retrieved content is tested also. We investigated different uses of the rating system, especially the impact of different ways of exchanging ratings and considering this first and second hand information for downloading decisions. Further aspects to study among others are the reliable creation of new identities (avoiding the impact of sybill attacks), the bootstrapping of the entire system, and peer selection issues.

5. REFERENCES

[1] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine. Surviving attacks on disruption-tolerant networks without authentication. In *MobiHoc '07*, pages 61–70, New York, NY, USA, 2007. ACM.

[2] C. Castelluccia and G. Montenegro. Protecting aodv against impersonation attacks. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(3):108–109, 2002.

[3] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft. Distributed community detection in delay tolerant networks. In *MobiArch '07*, pages 1–8, NY, USA, 2007. ACM.

[4] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *WWW '03*, pages 640–651, NY, USA, 2003. ACM.

[5] G. Karlsson, V. Lenders, and M. May. Delay-tolerant broadcasting. *Broadcasting, IEEE Transactions on*, 53(1):369–381, 2007.

[6] D. Quercia, S. Hailes, and L. Capra. Mobirate: making mobile raters stick to their word. In *UbiComp '08*, pages 212–221, NY, USA, 2008. ACM.

[7] S. U. Rahman, U. Hengartner, U. Ismail, and S. Keshav. Practical security for rural internet kiosks. In *NSDR '08*, pages 13–18, NY, USA, 2008. ACM.

[8] S. Čapkun, J.-P. Hubaux, and L. Buttyán. Mobility helps peer-to-peer security. *IEEE Transactions on Mobile Computing*, 5(1):43–51, 2006.

[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman. Sybilguard. *Networking, IEEE/ACM Transactions on*, 16(3):576–589, 2008.