

Distributed Security: Ad Hoc Networks & Beyond

Konrad Wrona

Abstract—Security is a factor of an increasing importance in the design of modern communications systems. This is especially true for decentralized communications systems like wireless ad hoc networks. The paper discusses security requirements for wireless ad hoc networks and gives an overview of related research projects.

I. OVERVIEW OF SECURITY REQUIREMENTS

Ad hoc networking has been a field of very active research in recent years. However, most of the research has been focused around various protocols for multi hop routing, leaving the area of security mostly unexplored.

At the same time, new applications of ad hoc networking, including wireless sensor networks, ubiquitous computing and peer-to-peer applications, introduce a need for strong privacy protection and security mechanisms.

High level security requirements for ad hoc networks are basically identical to security requirements for any other communications system, and include following services:

- authentication
- confidentiality
- integrity
- non-repudiation
- access control
- availability

However, similar to wireless communication systems creating additional challenges for implementation of aforementioned services when compared to fixed networks, ad hoc networks can be viewed as even more extreme case, requiring even more sophisticated, efficient and well designed security mechanisms, (5; 8; 10; 11). These additional challenges are caused by two basic assumptions of an ad hoc system:

- 1) lack of the infrastructure, and
- 2) a very dynamic and ephemeral character of the relationships between the network nodes.

The lack of infrastructure implies that there is no central authority, which can be referenced when it comes to making trust decisions about other parties in the network and that accountability can not be easily implemented. The transient relationships do not help in building trust based on direct reciprocity and give additional incentives to nodes to cheat.

Ad hoc networks rely on cooperation of involved nodes in order for the network to emerge and operate. Current versions of mature ad hoc routing algorithms only detect if the receiver's network interface is accepting packets, but they otherwise assume that routing nodes do not misbehave. Whereas such an assumption may be justified where single domain networks are

concerned, it is not easy to transpose it on a network consisting of nodes, unknown to, and untrusted by, each other. Since ad hoc networks deploy multi hop routing protocols, where each of the nodes in addition to its own packets has to forward packets belonging to other nodes, selfish behavior may represent a significant advantage for a node, saving his battery power and reserving more bandwidth for its own traffic. However, if a large number of nodes start to behave non-cooperatively, the network may break down completely, depriving all users of services. Non-cooperative behavior in multi hop routing protocols may also result in a denial of service attacks on the network, where the malicious nodes join the network for a sole reason of misbehaving and depriving all other nodes of legitimate services. Such denial-of-service focused misbehavior may consist of dropping (not forwarding) the packets, injecting incorrect routing information, replaying expired routing information or distorting routing information in order to partition the network, (6). Also bogus nodes may try to attract as much traffic as possible to themselves in order to be able to analyze it. In general, attacks on a routing protocol can be classified as, (2):

- non forwarding
- traffic deviations and route modifications
- lack of error messages
- frequent route updates.

Finding efficient solution to these problems in an open ad hoc environment is still an open issue.

At the same time, the confidentiality of transported data, which is one of the most commonly mentioned security problems in wireless systems, can be easily solved once the authentication and key sharing mechanisms are in place. Similar considerations apply to integrity protection, with integrity of the data stored in the devices being the most challenging issue.

Mobile, battery powered, devices always provide a constrained computational environment, when compared to fixed terminals. This is especially true in case of small wireless sensing devices and distributed personal networks. Also embedded intelligence and ubiquitous computing applications, even if free of power consumption considerations, will require cheap processors, with limited computational abilities. Small processors are often too slow for computationally intensive public-key cryptography. In the mobile environment, solving this problem by means of pre-computation or background task is not a solution, since the battery capacity puts an ultimate limit on the amount of computation which devices can perform. Thus, for the battery powered devices, the most relevant performance figure is no longer bits per second, but bits per joule, (9).

One of the biggest challenges in the area of confidentiality is not protecting the data transported by the network, but protecting the data stored on a device itself. Building tamper resistant and cost effective devices has turned out to be a challenge,

with most portable devices providing low security against data extraction. The smart card industry has driven most of the research in the area of tamper resistance, with some remarkable results. The problem of tamper resistance is especially valid in case of devices located outside the direct control of the owner, e.g. wireless sensors. Extracting the information stored in the device may lead to both compromise of the user's privacy and to impersonation attacks. The extracted authentication information from a remote sensor may enable an imposter to send the false sensing information or to block sending of the correct data. These kinds of attack can be avoided to some extent by using redundant information sources and communications routes and by applying voting mechanisms.

Another challenge is metadata protection, including confidentiality of identity (pseudonymity and anonymity), confidentiality of location (traceability) and traffic analysis. The confidentiality of this metadata will gain in importance in the ubiquitous computing environment, where the ubiquitous computing infrastructure could potentially become a tool for a powerful surveillance, making us involuntary participants in a world-wide *Big Brother* show.

The most common attacks on wireless communication systems consist of jamming the communication channel. This area has been studied intensively for military applications and most of the results can be applied also to civil networks.

A more dangerous attack in civil applications, typically using an open ad hoc environment, may consist of so-called *sleep deprivation torture*. In this type of denial-of-service attack, the attacker is trying to deprive a device of battery power, by keeping it awake and engaging in the communication all the time. A similar effect may be also caused by the device falling victim to parasitic computing applications, (1). Strong authentication of communication peers or some kind of accountability, based on either expensive pseudonyms and reputation mechanisms or micropayments, (3; 5), could be used to prevent this kind of attack to some extent. Micropayments could have form of both fungible payments, having monetary value, or infungible payments, e.g. crypto puzzles, (7). In more advanced scenarios, infungible micropayments could be harvested in order to perform some useful computations in a distributed way, similar to SETI@home concept.

In some scenarios, ad hoc networked devices may be required to form a distributed computation environment, e.g. in order to perform an analysis of collected data. Unfortunately, distributed computation environments introduce an inherent problem of efficient verification of obtained results, (4).

Data freshness is a security consideration in some applications, where a message reply attack might be possible. This applies to freshness of both application data (e.g. sensor readings) and freshness of signalling information (e.g. time synchronization within the network).

II. RESEARCH ROADMAP

The most interesting and least explored areas of ad hoc security include accountability, trust management, authentication and key management. Accountability and trust management pose new research problems because of the transient and decentralized nature of typical ad hoc networks. Some of the

problems in this area, especially concerning trust metrics and reputation mechanisms have already been encountered and to some extent solved in multi-agent systems and distributed artificial intelligence applications. Also, applying game theoretical analysis and mechanism design techniques, from modern microeconomics and cooperation theory, could be a promising approach to design of ad hoc communications systems.

Secure group forming, membership management and trust management, both within the group and between different groups, can be vital issues for some ad hoc applications, especially when using peer-to-peer platforms like JXTA. Some of the problems in this area are similar to the problems researched in case of the Internet multicast and group applications, though efficiency requirements are much more demanding in wireless ad hoc networks, as it was noted above.

Another open issue is a question of finding a compromise between anonymity and accountability, e.g. by applying expensive pseudonyms or fungible and infungible micropayments as a form of accountability. Use of the correctly designed incentive mechanism can also encourage the users to keep their nodes turned on and to refrain from sending a large amount of packets. It is also an interesting research problem how to reuse as much as possible of the computations performed by the device for different purpose, though such an approach can lead to new security challenges in itself. On the other hand, implementing mechanisms guarding against such reuse without participant's consent, i.e. parasitic computation, may be an important issue, too.

A key research objective in the area of authentication and key management in ad hoc networks is designing cryptographic mechanisms, which are efficient in sense of both computational and message overhead. In some cases, e.g. wireless sensing, designing efficient cryptographic mechanisms for authentication and key management in broadcast and multicast scenarios may pose a challenge.

The data confidentiality and integrity issues, can be tackled by re-using existing and efficient symmetric cryptographic algorithms, once the key management and authentication infrastructure is in place. Therefore there is no need for developing any special integrity and encryption algorithms for ad hoc networks.

Designing self-enforcing privacy policies and privacy enhancing mechanisms is a definite challenge for ubiquitous computing environments, with very little research done in this area so far.

REFERENCES

- [1] Albert-László Barabási, Vincent Freeh, Hawoong Jeong, and Jay Brockman, *Parasitic computing*, Nature **412** (2001), no. 30 Aug., 894–897.
- [2] Sonja Buchegger and Jean-Yves Le Boudec, *Performance analysis of the CONFIDANT protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)*, Proceedings of MOBIHOC'02 (EPFL Lausanne, Switzerland), ACM, June 9-11 2002.
- [3] Levente Buttyán and Jean-Pierre Hubaux, *Stimulating cooperation in self-organizing mobile ad hoc networks*, Technical Report DSC/2001/046, Swiss Federal Institute of Technology, Lausanne, Switzerland, July 31 2001.
- [4] Philippe Golle and Ilya Mironov, *Uncheatable distributed computations*, Proceedings of CT-RSA 2001, Lecture Notes in Computer Science, vol. 2020, Springer-Verlag, 2001, pp. 425–440.
- [5] Jean-Pierre Hubaux, Levente Buttyán, and Srdan Capkun, *The quest for security in mobile ad hoc networks*, Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC) (Long Beach, CA), ACM, Oct. 2001.
- [6] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, *Mitigating routing misbehavior in mobile ad hoc networks*, Mobile Computing and Networking, 2000, pp. 255–265.
- [7] Andy Oram, *Peer-to-peer: Harnessing the power of disruptive technologies*, O'Reilly, 2001, ISBN: 0-596-00110-X.
- [8] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J. D. Tygar, *SPINS: Security protocols for sensor networks*, 7th ACM International Conference on Mobile Computing and Networking (Rome, Italy), vol. 1, ACM Press, 2001, pp. 189–199.
- [9] Frank Stajano and Ross Anderson, *The resurrecting duckling: Security issues for ubiquitous computing*, IEEE Computer Magazine (2002), 22–26, Security and Privacy: Building Confidence in a Networked World (Supplement to IEEE Computer Magazine).
- [10] Seung Yi, Prasad Naldurg, and Robin Kravets, *Security-aware ad hoc routing for wireless networks*, Technical Report UIUCDCS-R-2001-2241, UIUC, 1304 West Springfield Avenue, Urbana, IL 61801-2987, USA, Aug. 2001.
- [11] Lidong Zhou and Zygmunt Haas, *Securing ad hoc networks*, IEEE Network Magazine **13** (1999), no. 6.