Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts Against Malice and Selfishness *

Sonja Buchegger
IBM Research, Zurich Research Laboratory
CH-8803 Rüschlikon, Switzerland
sob@zurich.ibm.com

Jean-Yves Le Boudec
EPFL-DSC-LCA
CH-1015 Lausanne, Switzerland
jean-yves.leboudec@epfl.ch

Abstract: In mobile ad-hoc networks, nodes do not rely on any routing infrastructure but relay packets for each other. Thus communication in mobile ad-hoc networks functions properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate, for example to save power or to launch security attacks such as denial-of-service. In this paper, we give an overview of potential vulnerabilities and requirements of mobile ad-hoc networks, and of proposed prevention, detection and reaction mechanisms to thwart attacks.

1 Introduction

In order to customize security and cooperation solutions for the requirements of various types of mobile ad-hoc networks, we make the following distinctions.

Closed vs. open world assumption. Mobile ad-hoc networks can be either managed by an organization that enforces access control or they can be open to any participant that is located closely enough.

Prevention vs. detection and reaction mechanisms. According to Schneier [Sch00], a prevention-only strategy will only work if the prevention mechanisms are perfect; otherwise, someone will find out how to get around them. Most of the attacks and vulnerabilities have been the result of bypassing prevention mechanisms. In view of this reality, detection and response are essential. In this paper we present proposals representing all of these classes.

Malicious vs. selfish behavior. As there is no infrastructure in mobile ad-hoc networks, the nodes have to cooperate in order to communicate. Intentional non-cooperation is mainly caused by two types of nodes: selfish ones that, e.g., want to save power, and malicious nodes that are not primarily concerned with power saving but that are interested in attacking the network.

The remainder of the paper is organized as follows. In Section 2 we state the problem,

* Proceedings of Mobile Internet Workshop. Informatik 2002., Dortmund, Germany, October 2002

followed by a brief overview of current solution proposals for either prevention or detection/reaction mechanisms in Section 3, and we conclude in Section 4.

2 Security and Cooperation Issues in Mobile Ad-hoc Networks

Mobile ad-hoc networks have properties that increase their vulnerability to attacks. **Unreliable wireless links** are vulnerable to jamming and by their inherent broadcast nature facilitate eavesdropping. **Constraints in bandwidth**, **computing power**, and **battery power** in mobile devices can lead to application-specific trade-offs between security and resource consumption of the device. **Mobility/Dynamics** make it hard to detect behavior anomalies such as advertising bogus routes, because routes in this environment change frequently. **Self-organization** is a key property of ad-hoc networks. They cannot rely on central authorities and infrastructures, e.g. for key management. **Latency** is inherently increased in wireless multi-hop networks, rendering message exchange for security more expensive. **Multiple paths** are likely to be available. This property offers an advantage over infrastructure-based local area networks that can be exploited by diversity coding.

Besides **authentication**, **confidentiality**, **integrity**, **availability**, **access control**, and **non-repudiation** being harder to enforce because of the properties of mobile ad-hoc networks, there are also additional requirements such as **location confidentiality**, **cooperation fairness** and the **absence of traffic diversion**.

The lack of infrastructure and of an organizational environment of mobile ad-hoc networks offers special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior; preventing someone else from getting proper service, extracting data to get confidential information, and so on.

Routes should be advertised and set up adhering to the routing protocol chosen and should truthfully reflect the knowledge of the topology of the network. By diverting the traffic towards or away from a node, incorrect forwarding, no forwarding at all, or other non-cooperative behavior, nodes can attack the network. Several routing and forwarding attacks have been described, e.g., in [BB01] and [HPJ01].

3 An Overview of Proposed Solutions

3.1 Prevention Mechanisms

Authentication by 'imprinting'. Stajano and Anderson [SA99] authenticate users by 'imprinting' in analogy to ducklings acknowledging the first moving subject they see as their mother, but enable the devices to be imprinted several times. Imprinting is realized by accepting a symmetric encryption key from the first device that sends such a key. They neither address routing nor forwarding, however, user authentication and authorization are

an important prerequisite for trust in the network layer also in mobile ad-hoc networks.

Asynchronous threshold security has been employed by Zhou and Haas [ZH99] together with share refreshing for distributed certification authorities for key management in mobile ad-hoc networks. They take advantage of inherent redundancies in such networks due to multiple routes to enable diversity coding, allowing for Byzantine failures given by several corrupted nodes or collusions. This approach potentially is a strong prevention mechanism, however, to the best of our knowledge, the impact on the network and the security performance remain to be investigated.

Incentives to cooperate have been proposed by Buttyán and Hubaux [BH00] in the form of so-called nuglets that serve as a per-hop payment in every packet or in the form of counters [BH01] to encourage forwarding. Both nuglets and counters reside in a secure module in each node, are incremented when nodes forward for others and decremented when they send packets for themselves. One of their findings is that, given such a module, increased cooperation is beneficial not only for the entire network but also for individual nodes.

Self-organized PGP by using chains of certificates has been developed by Hubaux, Buttyán and Capcun [HBC01]. Several certificate paths can be found by sharing information of nodes that each keep a small part of the certification knowledge, a prerequisite being the assumption that trust is transitive.

Localized certification based on the public key infrastructure (PKI) with certification-authority and secret-share update functionalities distributed among neighbors have been suggested by Kong, Zerfos, Luo, Lu and Zhang [KZL+01]. For threshold secret-sharing and certification nodes need K one-hop neighbors within a given time window. The nodes locally store the system certification revocation list. A simulation showed a good success ratio and tolerable delay.

SRP, the Secure Routing Protocol by Papadimitratos and Haas [PH02], guarantees correct route discovery, so that fabricated, compromised, or replayed route replies are rejected or never reach the route requester. SRP assumes a security association between end-points of a path only, so intermediate nodes do not have to be trusted for the route discovery. This is achieved by requiring that the request along with a unique random query indentifier reach the destination, where a route reply is constructed and a message authentication code is computed over the path and returned to the source. The correctness of the protocol is proven analytically.

ARIADNE, a secure on-demand routing protocol by Hu, Perrig, and Johnson [HPJ01], prevents attackers from tampering with uncompromised routes consisting of uncompromised nodes. It is based on Dynamic Source Routing (DSR) and relies on symmetric cryptography only. It uses a key management protocol called TESLA that relies on synchronized clocks. Simulations have shown that the performance is close to DSR without optimizations.

SEAD, Secure Efficient Distance vector routing for mobile ad-hoc networks by Hu, Johnson and Perrig [HJP02] is based on the design of destination-sequenced distance-vector routing (DSDV) and uses one-way hash functions to prevent uncoordinated attackers from creating incorrect routing state in another node. Performance evaluation has shown that

SEAD outperforms DSDV-SQ in terms of packet delivery ratio, but SEAD adds overhead and latency to the network.

3.2 Detection and Reaction

Intrusion detection for wireless ad-hoc networks has been proposed by Zhang and Lee [ZL00] to complement intrusion-prevention techniques. The authors argue that an architecture for intrusion detection should be distributed and cooperative, using statistical anomaly-detection approaches and integrating intrusion-detection information from several networking layers. They use a majority voting mechanism to classify behavior by consensus. Responses include re-authentication or isolation of compromised nodes. Detection rates and performance penalties remain to be investigated.

Watchdog and pathrater components to mitigate routing misbehavior have been proposed by Marti, Giuli, Lai and Baker [MGLB00]. They observed increased throughput in mobile ad-hoc networks by complementing DSR with a *watchdog* for detection of denied packet forwarding and a *pathrater* for trust management and routing policy rating every path used, which enable nodes to avoid malicious nodes in their routes as a reaction. Although this reaction does not punish malicious nodes that do not cooperate and actually relieves them of the burden of forwarding for others while having their messages forwarded, it allows nodes to use better paths and thus to increase their throughput.

CONFIDANT (see our papers [BB01], [BB02a], [BB02b]) stands for 'Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks' and it detects malicious nodes by means of observation or reports about several types of attacks and thus allows nodes to route around misbehaved nodes and to isolate them from the network. Nodes have a *monitor* for observations, *reputation records* for first-hand and trusted second-hand observations, *trust records* to control trust given to received warnings, and a *path manager* for nodes to adapt their behavior according to reputation. Simulations for "no forwarding" have shown that CONFIDANT can cope well even with half of the network population acting maliciously.

CORE, a collaborative reputation mechanism proposed by Michiardi and Molva [MM02], also has a *watchdog* component; however it is complemented by a sophisticated reputation mechanism that differentiates between subjective reputation (observations), indirect reputation (positive reports by others), and functional reputation (task-specific behavior), which are weighted for a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. Reputation values are obtained by regarding nodes as requesters and providers, and comparing the expected result to the actually obtained result of a request. A performance analysis by simulation is stated for future work.

4 Conclusion

Mobile ad-hoc networks are vulnerable to attacks that differ from those in fixed networks; their properties pose additional requirements to security and cooperation protocols. There

are many open research challenges, because by definition mobile ad-hoc networks are self-organized and have no infrastructure and central authorities. Examples for research questions are self-organized key management, cooperation incentives, group-membership and access control, authentication and identity persistence, and trust management.

References

[BB01] Sonja Buchegger and Jean-Yves Le Boudec. IBM Research Report: The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks. RR 3354, 2001.

[BB02a] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pages 403 – 410, Canary Islands, Spain, January 2002. IEEE Computer Society.

[BB02b] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Ad-hoc NeTworks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002.

[BH00] Levente Butty´an and Jean-Pierre Hubaux. Enforcing Service Availability in Mobile Ad-Hoc WANs. In *Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Boston, MA, USA, August 2000.

[BH01] Levente Butty´an and Jean-Pierre Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. Technical Report DSC/2001/046, EPFL-DI-ICA, August 2001.

[HBC01] J. Hubaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proceeding of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2001.

[HJP02] Yih-Chun Hu, David B. Johnson, and Adrian Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless AdHoc Networks. In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), IEEE, Calicoon, NY, to appear.*, June 2002.

[HPJ01] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks. Technical Report Technical Report TR01-383, Department of Computer Science, Rice University, December 2001.

[KZL+01] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks. In *International Conference on Network Protocols (ICNP)*, pages 251–260, 2001.

[MGLB00] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proceedings of MOBICOM 2000*, pages 255–265, 2000.

[MM02] Pietro Michiardi and Refik Molva. CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. Sixth IFIP conference on security communications, and multimedia (CMS 2002), Portoroz, Slovenia., 2002.

[PH02] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure Routing for Mobile Ad Hoc Networks. In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX*, January 2002.

[SA99] Frank Stajano and Ross Anderson. The Resurrecting Duckling. Lecture Notes in Computer Science, Springer-Verlag, 1999.

[Sch00] Bruce Schneier. *Secrets and Lies. Digital Security in a Networked World.* John Wiley & Sons, Inc, 1 edition, 2000.

[ZH99] Lidong Zhou and Zygmunt Haas. Securing Ad Hoc Networks. In *IEEE Network magazine, special issue on networking security, Vol. 13, No. 6, November/Dezember*, pages 24–30, 1999.

[ZL00] Yongguang Zhang and Wenke Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In *Proceedings of MOBICOM 2000*, pages 275–283, 2000.