[KGHS08] *André König, Christian Gottron, Matthias Hollick, Ralf Steinmetz;* **Harnessing Delay Tolerance to Increase Delivery Ratios in Mobile Ad Hoc Networks with Misbehaving Nodes.** In: Proceedings of the Fourth IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08), September 2008. Seite

Harnessing Delay Tolerance to Increase Delivery Ratios in Mobile Ad Hoc Networks with Misbehaving Nodes

André König, Christian Gottron, Matthias Hollick, Ralf Steinmetz
Multimedia Communications Lab (KOM), Technische Universität Darmstadt
{Andre.Koenig, Christian.Gottron, Matthias.Hollick, Ralf.Steinmetz}@KOM.tu-darmstadt.de

Abstract

Delay tolerant applications allow time to be used as an additional degree of freedom for security mechanisms in mobile ad hoc networks. By introducing artificial delays for the communication of delay tolerant applications, we optimize the point in time for starting or continuing a transmission. We develop mechanisms to exploit the knowledge on the proximity of the sender, the receiver, and intermediate, relaying nodes to misbehaving nodes detected. We propose different strategies for delayed transmission and provide a performance analysis based on a series of simulation studies. Our results show that we reduce the effects of misbehavior by keeping away data from misbehaving nodes.

1 Introduction

Mobile ad hoc networks (MANETs) enable enhanced communication services in scenarios which lack communication infrastructures. Networks to support on-site units in emergency response operations are a prominent application domain. Here, the availability of the network's services is a basic security demand. In contrast to this, the first communication protocols for MANETs were not designed for security but for functionality. As a result, attacks on these protocols are possible with little effort.

Cryptographic security mechanisms can achieve common security objectives such as confidentiality and authenticity. Yet, the basic availability of the network's services can only be assured up to a certain extent. Some of the most promising secure routing mechanisms for MANETs have been shown to be susceptible to attacks, recently in e.g. [1] or [2]. Furthermore, (most) secure routing mechanisms are not able to thwart misbehavior on other layers than the network layer. Jamming attacks, especially when performed in a sophisticated way as proposed in [7], can cause severe disruptions of network performance.

Intrusion detection systems (IDSs) in combination with intrusion response mechanisms can be deployed as a second line of defense for the case of subverted preventive measures. While IDSs for MANETs have been studied comprehensively, only minor attention has been paid to how to react to intrusions detected in the network. Mostly, address based response mechanisms have been proposed, which exclude adversaries from the network by not sending/receiving to/from addresses of misbehaving nodes. In [13] we have shown that this approach should not be the method of choice for MANETs where devices are usually beyond the control of a central instance and, thus, addresses can be changed with little effort. To deal with this, we have proposed *GeoSec* which uses space as an additional dimension for security mechanisms. With geographical quarantine zones we exclude misbehaving nodes from the network. Although this approach has shown to be immune against misbehaving nodes changing addresses, it is afflicted with inherent drawbacks. Two of the most severe being (A) benign nodes located within quarantine zones and, thus, excluded from the network and (B) routes between benign nodes outside quarantine zones that are interrupted due to the former. These cases are shown in Figure 1.

In this paper we describe how time can be used as a further dimension for security mechanisms to overcome the limitations of *GeoSec* stated above. By harnessing the delay tolerance of applications such as e-mail, we increase the reliability of a network (in terms of packets transmitted successfully) in the presence of multiple misbehaving nodes. After having discussed related work, we describe different strategies of how delay tolerant transmission can be realized. In a series of simulation studies we determine the trade-off between reliability and transmission delay.

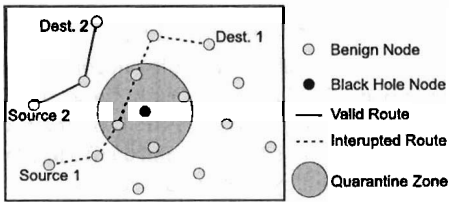


Figure 1. Side-effects of GeoSec

978-1-4244-2575-4/08/$20.00 ©2008 IEEE

2 Related Work

For our contribution presented here, the related work can be categorized into security related issues and into means for delay tolerant networking. Discussing the building blocks of MANETs is beyond the scope of this paper. For survey information, the reader may refer to [12].

2.1 Security Issues in MANETs

Attack possibilities in MANETs are manifold. In this paper, we focus on the black hole attack which has shown to have a devastating effect on network performance. Comparable to a black hole in astronomy which draws matter without escape (physicists may debate this definition), a black hole in a MANET draws data which is, subsequently, dropped instead of being forwarded to the receiver intended. The drawing effect of a black hole in a MANET is reached by pretending good routes regarding the metrics of the routing protocol deployed. Most likely, these routes will then be chosen instead of the 'honest' routes to the correct receiver.

As stated in the previous section, preventive security mechanisms for MANETs can be subverted. For this case, reactive security mechanisms can be deployed to form a second line of defense. For our needs, reactive mechanisms consist of IDSs in combination with intrusion response mechanisms.

An early approach to detect and react to misbehavior such as the black hole attack in MANETs has been proposed in [15]. Here, intrusion detection is performed by a component ('Watchdog') that makes use of the 802.11 promiscuous mode to monitor the forwarding behavior of neighboring nodes. Based on the assumption of symmetric wireless links, a node is able to overhear whether a neighbor relays packets correctly. With this information, nodes can be classified as benign or black holes.

Information obtained by IDSs is used by intrusion response mechanisms to penalize misbehaving nodes detected. Commonly, like in the cooperation enforcement schemes presented in [8], [16], and [4], this is done in an address-based way by not sending/receiving any data to/from these nodes. In [13], we have identified drawbacks of address-based intrusion response mechanisms as stated in Section 1. In consequence, we have proposed the location-based intrusion response mechanism *GeoSec* and compared its performance with an address-based approach.

2.2 Delay Tolerant Networking

Several approaches to enable delay tolerant communication have been proposed in literature. Out of these, we discuss Performance Enhancing Proxies (PEPs) [6], the Licklider Transmission Protocol (LTP) [17], and the Bundle Protocol [18] for potential deployment in our scenario.

PEPs in general split up connections into different sections each of which is optimized for the individual conditions of the corresponding network segment. PEP implementations exist on transport and application layer of the TCP/IP reference model. A well known example for a PEP on application layer is a proxy server for web browsing. Examples for PEP variants of TCP include snoop TCP [3] and Freeze-TCP [11]. TCP PEPs adapt TCP to the conditions in wireless environments in order to deal with lossy wireless channels and periodic disconnections.

LTP and the Bundle Protocol have been proposed by IRTF's Delay Tolerant Networking Research Group to enable efficient communication in disruptive environments as e.g. interplanetary networks. LTP resides above the data link layer and, thus, is designed to operate over one hop wireless links with very high delays in the scale of minutes up to hours. The Bundle Protocol works on an additional layer between transport and application layer. In a store-and-forward manner it takes data from application layer and uses common transport protocols like TCP or UDP to transmit the data (possibly over multiple hops) to the receiver intended as soon as the next hop in this direction is reachable. Together, LTP and the Bundle Protocol form a delay tolerant network stack, where LTP is responsible for reliable communication between adjacent nodes, and the Bundle Protocol provides end-to-end transmission.

To offer delay tolerant communication in our scenario, we have chosen to implement a simplified version of the Bundle Protocol. The combination with LTP as in the DTN architecture is not necessary since in our scenario, the wireless data link layer is based on the 802.11 protocol and, thus, is not subject to hight delays. Regarding disruption tolerance, also a PEP TCP variant would have been applicable. Yet, for reasons of flexibility regarding our future work, we have chosen not to be bound to TCP as transport protocol.

Security issues of DTNs have recently been studied in [9]. The authors scrutinize the inherent resistance against attacks of disruption tolerant networks.

3 Architecture

Our system consists of three components which become active consecutively. The intrusion detection component identifies and locates misbehavior ongoing. The intrusion response component establishes quarantine zones in areas where misbehavior has been detected. The delay tolerant networking component is responsible for the retransmission of packets that would have been dropped otherwise.

3.1 The Intrusion Detection System

For detection of the black hole attack, we use an approach that is comparable to the 'Watchdog' approach as described in Section 2.1. Detection is based on the rate with which a node drops packets that should have been forwarded. The steps performed are as follows:

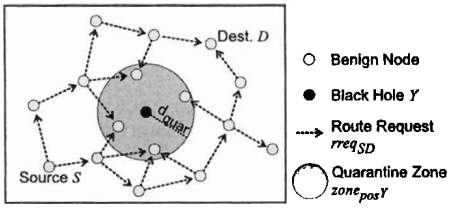


Figure 2. GeoSec's mode of operation

During a monitoring interval t_{mon}, a node X collects information about the forwarding behavior of its neighbors. We call a node Y a neighbor of a node X if X is within the transmission range of Y. For each of its neighbors, X maintains a counter c^Y_{rec} for packets that Y received from another neighbor of X or of X itself for forwarding. A second counter c^Y_{forw} is maintained for packets that Y forwarded to another neighbor Z or to X itself. Monitoring can be done buffered or unbuffered. In the unbuffered case, if Y turns out to be a black hole node, all packets that have been sent to Y during the monitoring interval t_{mon} are lost. In the buffered case, X temporarily stores the packets during each t_{mon}. If Y is classified as a black hole, the buffer content is handed to the Bundle Layer for retransmission. Otherwise, X flushes the buffer without further action.

After each monitoring interval t_{mon}, X calculates a rating r^X_Y that describes the forwarding behavior for each of its neighbors Y. We use a weighting factor $w_{balance} \geq 1$ to balance the counters c^Y_{rec} and c^Y_{forw}. With this, r^X_Y is calculated as $r^X_Y = \frac{c^Y_{rec}}{w_{balance}} - c^Y_{forw}$. If r^X_Y exceeds a certain threshold value $thres_{black}$, X classifies Y as a black hole.

3.2 The Intrusion Response Mechanism

The *GeoSec* intrusion response strategy excludes a black hole detected based on its location. If a node Y is classified as a black hole by a node X based on the rating r^X_Y, X establishes a quarantine zone $zone_{pos^Y}$ with a radius d_{quar} at Y's location pos^Y. If X is situated within $zone_{pos^Y}$, it will not forward any messages. Thus, also Route Request Messages that are usually sent as broadcast messages will not reach the Blackhole Y, as depicted in Figure 2. This way, we prevent Y from being a part of routes established newly while it is quarantined. At this point, we have to distinguish between transparent and non-transparent *GeoSec*. In the transparent case, if X is part of a route from a source S to a destination D, X will inform S by sending a corresponding Route Error Message. Thus, S is in duty to find a route to D which avoids the quarantine zone. All packets that are in flight or still sent by S until the Route Error Message arrives are handed to the Bundle Layer of X for future retransmissions. In the non-transparent case, X does not inform S about the quarantine zone established. Here, X hands all packets from S to the Bundle Layer and is completely responsible for finding new routes to D and retransmitting packets appropriately.

We assume that the tracking of nodes is not possible within a quarantine zone $zone_{pos^Y}$. Therefore an adaptation of $zone_{pos^Y}$ if Y moves is not possible. For this reason, a reset of a quarantine zone $zone_{pos^Y}$ is performed after a time $t^{zone_{pos^Y}}_{reset}$. If Y leaves the quarantine zone, it may again become part of routes and drop packets. Y is then classified as a Blackhole again and a new quarantine zone is established.

3.3 The Bundle Layer

The mode of operation of our implementation of the Bundle Protocol is shown in Figure 3. The Bundle Layer resides between transport layer and application layer as specified in [18]. Packets that would have been dropped by *GeoSec* due to quarantine zones established can be handed to the Bundle Layer for retransmission. This can be done at the sender as well as at each intermediate node. This way, also packets that are buffered by the IDS during a monitoring phase can be handed to the Bundle Layer if a black hole node has been detected.

The Bundle Layer is parameterized by the time span $t_{retrans}$ between two subsequent retransmission attempts and the number $n_{retrans}$ of retransmission attempts that are to be performed per packet. $n_{retrans}$ is a global value. The number of retransmission attempts left is (besides other information required) transmitted along with the user data in an additional Bundle Header.

4 Performance Evaluation

We now evaluate the mechanisms proposed in the previous section. We provide an analysis of the trade-off between transmission delay and ratio of packets delivered successfully in a MANET with multiple misbehaving nodes. We show a comparison of the performance of *GeoSec* with and without the support of the delay tolerant networking component. We consider the four combinations possible of transparent and non-transparent *GeoSec* as well as buffered and unbuffered IDS.

4.1 Metrics used for Evaluation

As primary metrics we use the ratio of packets delivered with the help of the Bundle Layer and the average trans-

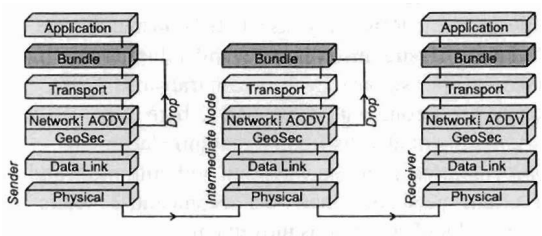


Figure 3. Bundle layer

mission delay of packets that have been delivered with the help of the Bundle Layer. These metrics are influenced directly by the configuration of the Bundle Layer and, thus, reflect the trade-off between transmission delay and ratio of packets successfully delivered.

As secondary metrics we use the ratio of packets dropped due to the black hole nodes and the intrusion response itself as well as the ratio of packets transmitted successfully and the transmission delay as it would be observed without the Bundle Layer. These metrics serve as basis for the comparison of the additional measures presented in this paper with the 'pure' *GeoSec* approach. Further secondary metrics that have shown not to be influenced by the specific configuration of the Bundle Protocol are the average route length and the ratio of packets dropped due to inherent network conditions such as collisions on the wireless medium.

4.2 Experimental Design

From the large amount of parameters that characterize the network (transmission power of nodes, antenna characteristics, traffic patterns, mobility models), we have chosen a small set of factors which considerably influence the performance with respect to our primary metrics used for evaluation. These factors are the number $n_{retrans}$ of retransmission attempts that are performed by the Bundle Layer and the time span $t_{retrans}$ between the individual retransmission attempts. We evaluate the mechanisms proposed by means of simulation. For this, we use the JiST/MobNet simulator as presented in [14]. JiST/MobNet is based on JiST/SWANS [5], which was reorganized and extended at our institute. Besides other functionality, we added attack variants and the security mechanisms as presented in Section 3. To improve runtime, we use a Condor cluster [10] for distributed computation of the simulations. The protocols deployed in the MANET are as follows:

- *Medium Access Layer:* IEEE 802.11 DCF
- *Network Layer:* IPv4 with AODV routing service
- *Transport Layer:* UDP

The basic parameters of the network are chosen as:

- *Benign nodes / black holes:* 990 / 10.
- *Transmission range:* 250 meters.
- *Average neighbors per node:* 7 - 8.
- *Resulting simulation area:* 4750 m · 4750 m.
- *Traffic pattern:* Randomly distributed constant bitrate traffic with 10 streams in parallel and a duration of 30 seconds per stream. Each stream transmits 4 packets per second with a size of 512 byte each.
- *Placement:* Equally distributed random placement.
- *Mobility model:* Random waypoint with minimum and maximum speeds of 1 meter per second and 2 meters per second and continuous movement.
- *Simulated time:* 1 hour for each factor set split up in 6 parts with 10 minutes each to distribute workload and reduce unwanted effects of the random waypoint mobility model.

We have chosen the parameters and factors such that we obtain a moderate network load, i.e. in average the network operates in a non-congested state. Some setups have shown to cause congestion situations. A more detailed discussion is provided in the following section.

We further have selected mobility of the nodes to correspond to pedestrian speed. With this, we achieve a reasonable lifetime of routes and, accordingly, a feasible overhead of routing messages w.r.t. to data messages.

To obtain a reasonable performance of the IDS, we chose a monitoring interval t_{mon} of 1 second and a weighting factor $w_{balance}$ of 10.

The quarantine radius d_{quar} for *GeoSec* is set to 250 meters according to the transmission range of nodes. The reset interval $t_{reset}^{zone_{posY}}$ is set to 300 seconds which has shown to be an optimal value in our experiments presented in [13].

The factors for evaluation are as follows:

- $n_{retrans}$: 1, 4, 8, 16, 32
- $t_{retrans}$ *in seconds:* 10, 20, 30, 40, 50, 60

For each combination of transparent and non-transparent *GeoSec* and buffered and unbuffered IDS, we have simulated all combinations of $n_{retrans}$ and $t_{retrans}$.

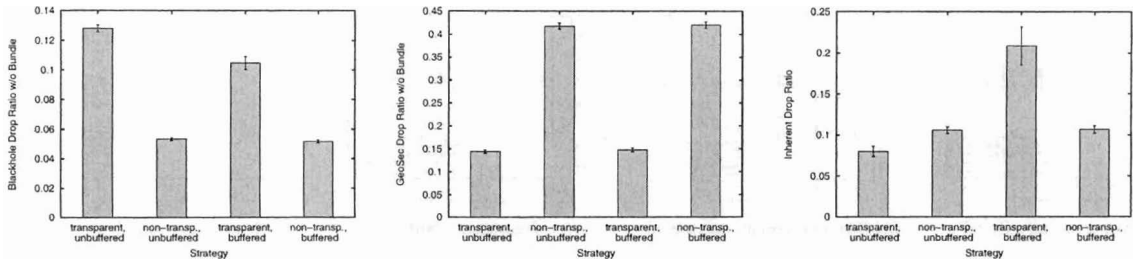
4.3 Presentation of the Results

In this section, we discuss the results of our simulation study. All plots are given with 95% confidence intervals.

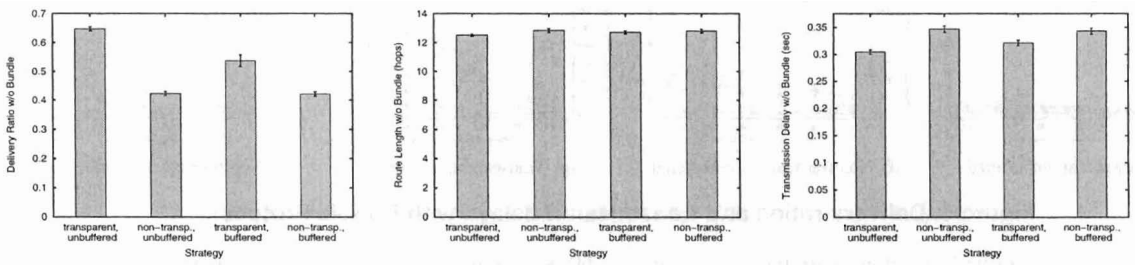
Figure 4 shows the results for the secondary metrics as defined in Section 4.1 which we use as basis for the performance evaluation of the delay tolerant networking component. Note that these metrics show the behavior of the network without the retransmissions of the Bundle Layer. The secondary metrics have shown no variations of statistical significance with respect to the individual factors selected in the previous section. Thus, the results presented in Figure 4 are the accumulated results of all simulation runs for the combinations of transparent and non-transparent *GeoSec* and buffered and unbuffered IDS.

What is remarkable is that the ratio of packets dropped by black holes as shown in Figure 4(a) significantly differs between transparent and non-transparent *GeoSec*. With about 5%, the non-transparent strategy shows to have a drop ratio of less than half that of the transparent version. The particular reason for this is still under evaluation. Note that in a defenseless network with 10 black hole nodes, we observe black hole drop ratios of more than 90%.

The ratio of packets dropped due to quarantine zones established in the network is shown in Figure 4(b). The high drop ratios of the non-transparent strategies are due to the fact that the sender is not informed about quarantine zones



(a) Average Black Hole Drop Ratio w/o Bundle (b) Average GeoSec Drop Ratio w/o Bundle (c) Average Inherent Drop Ratio



(d) Average Delivery Ratio w/o Bundle (e) Average Route Length per Packet (f) Average Transmission Delay w/o Bundle

Figure 4. Simulation results without or not subject to the Bundle Protocol

established. Thus, all packets arriving at the first node that is situated within a quarantine zone would be dropped if this strategy is not used in combination with the Bundle Layer.

The ratio of packets dropped due to inherent network conditions such as collisions on the wireless medium is shown in Figure 4(c). Remarkable here is the fact that transparent *GeoSec* in combination with the buffered IDS has an inherent drop ratio of about 20% which is more than twice the inherent drop ratio of other combinations. From the also quite large confidence intervals we conclude that this particular case causes a high network load which leads to congestion situations.

Figure 4(d) shows the ratio of packets delivered successfully without the Bundle Protocol. The delivery ratio is the difference between all packets sent and packets dropped due to black holes, *GeoSec*, and inherent network conditions.

The average route length and the average transmission delay are shown in Figures 4(e) and 4(f), respectively. Both metrics do not show significant differences for the individual strategies evaluated.

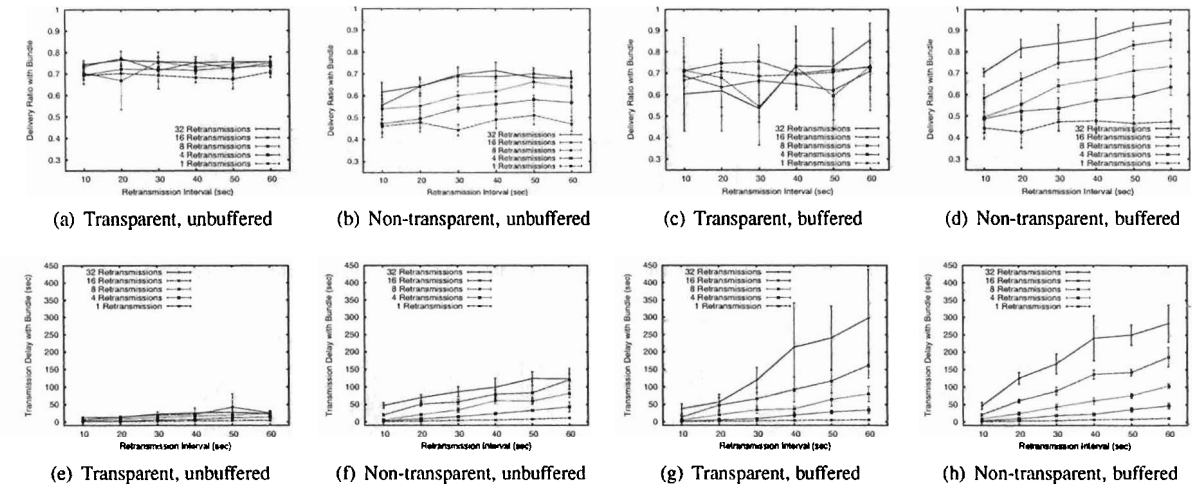
The average ratio of packets successfully transmitted with the help of the Bundle Layer is shown in Figures 5(a) to 5(d). Intuitively, the delivery ratio raises along with the number $n_{retrans}$ of retransmission attempts. For a fixed value of retransmission attempts, the delivery ratio raises (slightly) along with the time span $t_{retrans}$ between subsequent retransmission attempts. This is due to the fact that quarantine zones have a diameter of 500 meters. Compared to this size, nodes move at relatively low speed between 1 and 2 meters per second. Thus, the larger $t_{retrans}$, the larger is the probability that a node which has to retransmit packets has left the quarantine zone and can establish a route to the target successfully.

From Figure 4, we know that the number of packets that have to be retransmitted by the Bundle Layer is higher for the non-transparent than for the transparent strategies. Thus, the difference between the curve sets of the transparent strategies is smaller than for the non-transparent strategies. In both cases, we start from the corresponding number of packets delivered without the Bundle Layer as shown in Figure 4(d). The differences between the best values achieved can be explained by the ratio of packets dropped due to inherent network conditions which are not buffered by the Bundle Layer and, thus, are not retransmitted.

Intuitively, the delivery ratio is higher for the buffered than for the unbuffered IDS. The congestion situation we mentioned for the combination of transparent *GeoSec* and buffered IDS can be seen again from the unsteady trend and the large confidence intervals in Figure 5(c).

As a whole, we observe delivery ratios of about 90% in the best cases which means that all packets that would otherwise have been lost due to black holes or *GeoSec* itself were retransmitted successfully. Only packets that are lost due to inherent network conditions which can not be detected at the sender side and, thus, are not handed to the Bundle Layer for retransmission are lost.

The average transmission delay for packets transmitted successfully including retransmissions of the Bundle Layer is shown in Figures 5(e) to 5(h). For all strategies, the transmission delay raises along with the number of packets



(a) Transparent, unbuffered (b) Non-transparent, unbuffered (c) Transparent, buffered (d) Non-transparent, buffered

(e) Transparent, unbuffered (f) Non-transparent, unbuffered (g) Transparent, buffered (h) Non-transparent, buffered

Figure 5. Delivery ratios and transmission delays with Bundle Protocol

that have to be retransmitted and along with the number of retransmission attempts and the time span between subsequent retransmission attempts. As a whole, we buy higher delivery ratios for the price of higher transmission delays which can reach up to several minutes.

5 Conclusion & Outlook

In this paper we have shown how artificial transmission delays can be used to support security mechanisms in MANETs. By delaying transmissions and retransmissions appropriately, we keep data away from misbehaving nodes detected. We have proposed and evaluated different strategies on how transmissions can be delayed and buffered. Our simulation studies have shown that we are able to nearly recover the performance of a clean network with respect to the ratio of packets delivered. The price we have to pay for this (in our scenario) is a strong increase of the average transmission delay. Thus, our approach can be deployed for delay tolerant applications such as e-mail or short message services but is infeasible for real-time communication.

In our future work, we will examine how *GeoSec* can be further supported by an adaptive transmission power of nodes. With this, we will be able to reduce the size of quarantine zones. We expect a further improvement in *GeoSec*'s performance and flexibility.

References

[1] G. Acs et al. Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks. In *Proc. of ESAS '05*. July 2005.

[2] G. Acs, et al. Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing*, 5(11):1533–1546, 2006.

[3] H. Balakrishnan et al. Improving TCP/IP Performance over Wireless Networks. In *Proc. of MobiCom '95*, Nov. 1995.

[4] S. Bansal et al. Observation-based Cooperation Enforcement in Ad hoc Networks. TR, Stanford University, July 2003.

[5] R. Barr. *An Efficient, Unifying Approach to Simulation using Virtual Machines*. PhD thesis, Cornell University, 2004.

[6] J. Border et al. Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations. *IETF RFC 3135*, 2001.

[7] T. X. Brown et al. Jamming and Sensing of Encrypted Wireless Ad Hoc Networks. In *Proc. of MobiHoc '06*, May 2006.

[8] S. Buchegger. *Coping with Misbehavior in Mobile Ad-hoc Networks*. PhD thesis, École Polytechnique Fédérale de Lausanne, Feb. 2004.

[9] J. Burgess et al. Surviving Attacks on Disruption-Tolerant Networks without Authentication. In *Proc. of MobiHoc '07*, Sept. 2007.

[10] Dept. of Computer Science, University of Wisconsin - Madison. Condor Project Homepage. *http://www.cs.wisc.edu/condor*, Sept. 2007.

[11] T. Goff et al. Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environments. In *Proc. of INFOCOM 2000*, March 2000.

[12] Z. J. Haas et al. Wireless Ad Hoc Networks. In *Encyclopedia of Telecommunications*. John Wiley, 2002.

[13] A. König et al. GeoSec - Quarantine Zones for Mobile Ad Hoc Networks. *Submitted to Security and Communication Networks*, 2008.

[14] T. Krop et al. JiST/MobNet: Combined Simulation, Emulation and Real-World Testbed for Ad hoc Networks. In *Proc. of WiNTECH '07*, Sept. 2007.

[15] S. Marti et al. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proc. of MobiCom '00*, Aug. 2000.

[16] P. Michiardi et al. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In *Proc. of IFIP CMS '02*, Sept. 2002.

[17] M. Ramadas et al. Licklider Transmission Protocol - Specification. *IRTF Delay Tolerant Networking Research Group Internet-Draft*, draft-irtf-dtnrg-ltp-09.txt, 2008.

[18] K. Scott et al. Bundle Protocol Specification. *IETF RFC 5050*, 2007.

Security for Future Wireless and Decentralized Communication Networks – Harnessing Cooperation, Space, and Time

André König, Matthias Hollick, Ralf Steinmetz
[Andre.Koenig; Matthias.Hollick; Ralf.Steinmetz]@KOM.tu-darmstadt.de
Multimedia Communications Lab (KOM), Technische Universität Darmstadt

Wireless and decentralized networks enable enhanced communication services beyond the borderlines of 'traditional' centralized, infrastructure-based systems. As an example, projects have been initiated that scrutinize the applicability of a combination of mobile ad hoc networks (MANETs) and Peer-to-Peer (P2P) systems to support on-site units in highly dynamic emergency response scenarios. This new class of networks demands for new security mechanisms. Due to the wireless and infrastructureless nature, MANETs and P2P systems lack the well defined network borders and the central trusted instances on which security mechanisms (Gateways, Firewalls, etc.) deployed in 'traditional' environments are based. Thus, these security mechanisms cannot be transferred directly. In our work, we present security mechanisms that cope with the challenging conditions in wireless and decentralized systems. We show how cooperative decisions can counterbalance missing central instances and how networks being aware of space and time constraints can survive without well defined network borders.

I. Harnessing Cooperation

Security mechanisms that ensure objectives such as authentication and access control are commonly based on central trusted instances. In decentralized P2P systems, the (constant) availability of these central trusted instances cannot be taken as granted. Making security relevant decisions jointly, by a set of authorized peers, is a promising approach to counterbalance missing central trusted instances. This way, a security level that is comparable to that of contemporary security mechanisms can be achieved.

The mathematical foundation for a joint decision process is given by threshold cryptography or multisignatures. Both techniques can be utilized to enforce the cooperation of a specific number $n_{threshold}$ of peers to perform cryptographic operations such as signing certificates that enable the access to restricted resources. Threshold cryptography allows for anonymous voting, whereas multisignatures render the voting traceable and enable a detailed mapping of administrative hierarchies to the structure of the network.

Predefined security policies for any security relevant decision possible will most likely not be available regarding the highly dynamic application domain targeted. Thus, a user interaction may well be required. Minimizing the number $n_{request}$ of users requested for one joint decision is an obvious optimization goal. To describe the trade-off between $n_{request}$ and the probability p_{succ} that a joint decision is successful (i.e. enough peers w.r.t. $n_{threshold}$ issued their votes within a reasonable amount of time), as shown in Figure 1, we developed stochastic models. The derived closed-form description of these models serves as a tool allowing for the online adaptation of key parameters which control the success of joint decisions while guaranteeing low overhead in the network.

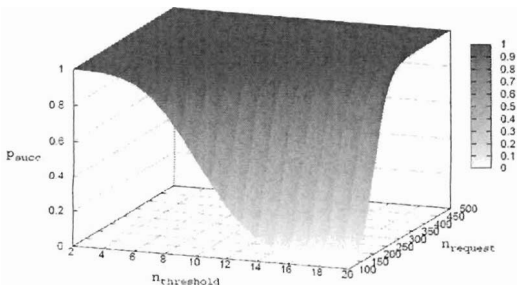


Figure 1: Success probability for cooperative decisions

II. Harnessing Space and Time

Establishing networks without an infrastructure, as it is done in a MANET, requires an accurate cooperation of the nodes involved. Effects of misbehaviour, may it be intended or not, can lead to a massive disruption of the network's services.

A prominent example of (intended) misbehaviour in MANETs is the black hole attack. In analogy to a black hole in astronomy, a black hole in a MANET draws data, which is dropped instead of being forwarded to the actual receiver. Very few of such black hole nodes are sufficient to cause a breakdown of the entire network.

Preventing any misbehaviour possible is hardly feasible. Prevention strategies, though thoroughly designed, have been shown to be susceptible to attacks, recently. However, reactive security measures like intrusion detection systems combined with intrusion response mechanisms offer a promising means to mitigate the effects of misbehaviour in MANETs. While intrusion detection systems have been studied comprehensively, only minor attention has been paid to how to react to intrusions detected. Mostly, response mechanisms which exclude adversaries detected from the network based on their addresses have been proposed. Since devices in MANETs are beyond the control of a central instance, changing addresses is possible with little effort. This way, address-based intrusion response approaches can be subverted easily. For this reason, we have proposed *GeoSec*, a location-based intrusion response strategy. By setting up temporal quarantine zones in areas where misbehaviour has been detected, network traffic is redirected and, thus, is geographically kept away from misbehaving nodes. Figure 2 shows *GeoSec*'s performance compared to a defenseless network and to an address-based response strategy, subject to the data that is dropped by black hole nodes.

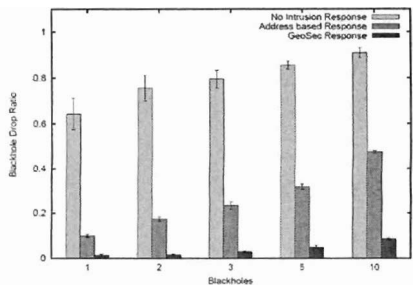


Figure 2: Address-based vs. location-based intrusion response

Kooperative Sicherheitsmechanismen für Peer-to-Peer Systeme – Varianten und Erfolgsmodelle

André König, Matthias Hollick, Ralf Steinmetz
[Andre.Koenig; Matthias.Hollick; Ralf.Steinmetz]@KOM.tu-darmstadt.de
FG Multimedia Kommunikation (KOM), Technische Universität Darmstadt

Neben dem Austausch von Daten als derzeitigem Hauptanwendungsgebiet bieten Peer-to-Peer (P2P) Systeme zahlreiche Möglichkeiten zur Entwicklung neuartiger wissenschaftlicher und kommerzieller Anwendungen. In Verbindung mit mobilen Ad hoc Netzen (MANETs) können z.B. Kommunikations- und Informationsdienste zur Unterstützung von Einsatzkräften in Katastrophenszenarien aufgebaut werden. Voraussetzung hierfür sind effektive und zuverlässige Sicherheitsmaßnahmen. Aufgrund der dezentralen Natur von P2P Systemen können aus Client-Server Umgebungen bekannte Sicherheitsmaßnahmen nicht (ohne umfangreiche Modifikation) in P2P Systemen angewendet werden. In diesem Beitrag präsentieren wir Sicherheitsmechanismen, die durch den Einsatz kooperativer Entscheidungen für P2P Systeme geeignet sind. Mittels statistischer Modelle beschreiben wir die Funktionsweise verschiedener Kooperationsvarianten.

I. Motivation und Ziele

P2P Systeme ermöglichen den Aufbau von Kommunikations- und Informationsdiensten ohne den Einsatz zentraler Komponenten (Server). MANETs ermöglichen den Aufbau von Netzen ohne Infrastruktur. Durch eine Kombination beider Technologien können z.B. spontane Netze zur Unterstützung von Polizei- und Rettungskräften in Katastrophenszenarien zur Verfügung gestellt werden. Die in diesem Beitrag diskutierten Sicherheitsmechanismen werden im Hinblick auf die Eignung für den Einsatz in solchen vollständig dezentralen und infrastrukturlosen Systemen untersucht. Verwandte Arbeiten in diesem Bereich sind z.B. die Projekte DUMBO [1] und HiMONN [2]. Gerade in dem skizzierten Anwendungsszenario sind effektive, grundlegende Sicherheitsmaßnahmen wie Nutzerauthentifizierung und Zugangskontrolle von besonderer Bedeutung, um den Zugriff auf das Netz selbst und die zur Verfügung gestellten Dienste und Informationen zu schützen. Herkömmliche, in Client-Server Systemen eingesetzte Mechanismen zur Authentifizierung und Zugangskontrolle wie z.B. Kerberos [3] basieren auf zentralen, vertrauenswürdigen Instanzen. In P2P Systemen sind solche zentralen, vertrauenswürdigen Instanzen (per Definition) nicht vorhanden. Existierende Mechanismen zur Authentifizierung und Zugangskontrolle können deshalb nicht (ohne umfangreiche Modifikation) in P2P Systemen eingesetzt werden.

Um ein mit Client-Server Systemen vergleichbares Sicherheitsniveau zu erreichen, können sicherheitsrelevante Entscheidungen (Nutzerauthentifizierung, Zugangskontrolle) in P2P Systemen in Kooperation mehrerer, dazu autorisierter Peers getroffen werden. So kann verhindert werden, dass einzelne, evtl. kompromittierte Peers die Sicherheit des Systems gefährden. In diesem Beitrag stellen wir verschiedene Varianten dieser kooperativen Entscheidungen vor. Weiterhin präsentieren wir statistische Modelle, die den kooperativen Entscheidungsprozess bzgl. verschiedener Systemparameter wie z.B. der Paketverlustrate im Netz oder der für eine Entscheidung benötigten Anzahl zustimmender Peers beschreiben.

II. Kryptographische Grundlagen

mathematische Fundament zur Realisierung kooperativer Entbilden Schwellwertkryptographie und Multisignaturen. Beide Verfahren basieren (für unsere Zwecke) auf asymmetrischer Kryptographie und werden im Folgenden abstrakt beschrieben.

Für den Einsatz von Schwellwertkryptographie wird ein (privater) Signaturschlüssel S in mehrere Teilschlüssel S_i aufgeteilt. Hierfür wird, wie in Abbildung 1 dargestellt, ein Polynom $p(x)$ so gewählt, daß $S=p(0)$ gilt. Die Teilschlüssel entsprechen dann Funktionswerten des Polynoms an bestimmten Indexstellen, also $S_i=p(i)$ mit $i\neq 0$. Dieses Verfahren wurde zuerst in [4] beschrieben. Jeder entscheidungsberechtigte Peer P_i erhält den entsprechenden Teilschlüssel S_i. Soll nun z.B. ein Zertifikat Z signiert werden, dass einem Peer P den Zugang zu Diensten im P2P System ermöglicht, können die Inhaber P_i der Teilschlüssel S_i (falls sie zustimmen) teilsignierte Zertifikate Z_i erstellen. Mittels Lagrange-Interpolation kann P das vollständig signierte Zertifikat Z aus den teilsignierten Zertifikaten Z_i berechnen. Je nach Grad des Polynoms $p(x)$ (dem Schwellwert) werden hierfür entsprechend viele teilsignierte Zertifikate benötigt.

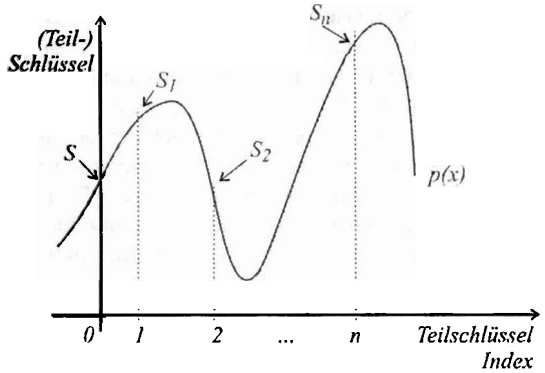


Abb. 1: Teilschlüsselerzeugung für Schwellwertkryptographieverfahren

Unterschieden wird zwischen interaktiven und nicht-interaktiven Schwellwertsignaturverfahren. Im Gegensatz zu nicht-interaktiven Verfahren benötigen interaktive Verfahren während des Erzeugens der Teilsignaturen eine Kommunikation (in evtl. mehreren Runden) der beteiligten Peers. Aufgrund der inhärenten Bedingungen in MANETs (relativ hohe Paketverlustraten, evtl. temporär unerreichbare Netzteilnehmer) sind interaktive Verfahren für den Einsatz in unserem Anwendungsszenario nicht geeignet. Ein geeignetes, nicht-interaktives Verfahren wird z.B. in [5] beschrieben.

Anhand einer mittels Schwellwertkryptographie erzeugten Signatur kann keine Information über die verwendeten Teilschlüssel S_i und damit über die an einer Entscheidung beteiligten Peers P_i gewonnen werden. Soll die Identifizierung der beteiligten Entscheidungsträger anhand der Signatur möglich sein oder die Menge der entscheidungsberechtigten Peers auf bestimmte Peers eingeschränkt werden, können Multisignaturen an Stelle von Schwellwertkryptographie als Basis für kooperative Entscheidungen verwendet werden. Jeder Peer besitzt dafür ein eigenes, an seine Identität gebundenes (asymmetrisches) Schlüsselpaar. In der einfachsten Variante wird eine vollständige Signatur durch die Verkettung der Identitäten der einzelnen Signierer sowie den entsprechenden Signaturen erzeugt. Hierbei steigt allerdings sowohl die Länge der Gesamtsignatur als auch die zur Verifikation benötigte Zeit linear mit der Anzahl der Teilsignaturen. Da in unserem Anwendungsszenario die zur Verfügung stehende Rechenleistung der beteiligten Geräte und die Bandbreite des Netzes beschränkt sind, sind diese einfachen Multisignaturverfahren nicht geeignet. Komplexere Multisignaturverfahren erzeugen eine komprimierte Signatur aus den Teilsignaturen ohne Informationsverlust. Unterschieden wird wieder zwischen interaktiven und nicht-interaktiven Verfahren. Analog zu Schwellwertverfahren sind interaktive Multisignaturverfahren nicht für den Einsatz in unserem Anwendungsszenario geeignet. Ein geeignetes, nicht-interaktives Verfahren wird z.B. in [6] beschrieben.

III. Struktur vs. Chaos

Soll eine kooperative Entscheidung getroffen werden, müssen entsprechende Anfragen an mehrere Entscheidungsträger gestellt werden. Die Strategie, die zum Versenden dieser Anfragen genutzt wird, hat direkten Einfluss auf die erzeugte Netzlast und die Erfolgswahrscheinlichkeit, d.h. auf die Wahrscheinlichkeit, eine ausreichende Anzahl von Antworten zu erhalten um eine vollständige Signatur berechnen zu können.

Eine einfache Strategie ist, Anfragen direkt von einem Peer, der z.B. den Zugriff auf einen Dienst beantragt, als Broadcast im P2P System zu versenden. Dieser Ansatz wird in [7] zur Regelung des Zugangs zu geschlossenen Benutzergruppen vorgeschlagen. Jeder Empfänger der Anfrage kann, sofern er Inhaber eines Teilschlüssels ist, ein teilsigniertes Mitgliedschaftszertifikat für die Benutzergruppe ausstellen. Aufgrund der durch den Broadcast der Anfragen erzeugten Netzlast ist diese Strategie für unser Anwendungsszenario nur bedingt geeignet. Um die durch eine kooperative Entscheidung erzeugte Netzlast möglichst gering zu halten, verwenden wir deshalb zwei alternative Anfragestrategien. Durch einen beschränkten Broadcast kann die Netzlast deutlich verringert werden. Anfragen werden hier ebenfalls direkt von dem anfragenden Peer an (potentielle) Entscheidungsträger gesendet. Die Einschränkung des Broadcasts kann dabei z.B. durch statistische Methoden oder durch eine Beschränkung auf die geographische Umgebung des anfragenden Peers erfolgen. Da wir annehmen, dass in unserem Anwendungsszenario die Anzahl der entscheidungsberechtigten Peers aus administrativen Gründen gering ist, führt ein eingeschränkter Broadcast evtl. nicht zum Erfolg. Dies ist vor allem dann der Fall, wenn dem anfragenden Peer die Teilschlüsselinhaber nicht bekannt sind. Für diesen Fall verwenden wir eine koordinierte Anfragestrategie. Ein dedizierter Peer übernimmt dabei die Rolle als Ansprechpartner / Verteiler für sicherheitsrelevante Entscheidungen. Dieser Peer hat Kenntnis über die Teilschlüsselinhaber und kann so gezielt Anfragen stellen. Da die Rolle des Koordinators von einem beliebigen Peer übernommen werden kann, widerspricht dieses Modell nicht der Definition von P2P Systemen.

IV. Erfolgsmodelle

Durch inhärente Bedingungen in unserem Anwendungsszenario (Paketverluste im MANET, Peers temporär nicht erreichbar) können gestellte Anfragen und Antworten verloren gehen. Trotzdem soll sowohl die Zeit zwischen einer gestellten Anfrage und dem Erhalt einer ausreichenden Zahl von Antworten als auch die durch (evtl. notwendige wiederholte) Anfragen erzeugte Netzlast möglichst gering gehalten werden. Um dies zu erreichen kann eine gewisse Menge überschüssiger Anfragen bzgl. der benötigten Anzahl an Antworten um eine vollständige Signatur erzeugen zu können durchaus sinnvoll sein. Im Folgenden beschreiben wir die Erfolgswahrscheinlichkeit p_E, also die Wahrscheinlichkeit nach einer Anfrage eine ausreichende Zahl von Antworten zu erhalten bzgl. der Anzahl n_G der gesamten Peers im P2P System, der Antwortwahrscheinlichkeit p_A einzelner Teilschlüsselinhaber, der Anzahl n_A der Peers, an die eine Anfrage gesendet wurde sowie der Anzahl n_T der benötigten Antworten um eine gültige Signatur erzeugen zu können.

Für den vollständigen Broadcast kann die Wahrscheinlichkeit $p(n_Z)$, eine bestimmte Anzahl n_Z von Antworten (teilsignierte Zertifikate) auf eine Anfrage zu erhalten als binomische Zufallsvariable beschrieben werden. Es gilt

$$p(n_Z) = \binom{n_G}{n_Z} \cdot p_A^{n_Z} \cdot (1-p_A)^{n_G - n_Z}$$

Eine Anfrage ist erfolgreich, wenn der anfragende Peer eine ausreichende Zahl von Antworten erhält, um eine vollständige Signatur erzeugen zu können, wenn also $n_Z \geq n_T$. Die Erfolgswahrscheinlichkeit p_E kann dementsprechend als Summe binomischer Zufallsvariablen beschrieben werden. Es folgt

$$p_E = p(n_Z \geq n_T) = \sum_{n_Z=n_T}^{n_G} \binom{n_G}{n_Z} \cdot p_A^{n_Z} \cdot (1-p_A)^{n_G - n_Z}$$

Der eingeschränkte Broadcast wird durch eine hypergeometrische Zufallsvariable dargestellt. Diese beschreibt die Schnittmenge der Peers, an die eine Anfrage gestellt wurde und der Peers, die potentiell auf eine Anfrage antworten würden. Die Erfolgswahrscheinlichkeit p_E wird als Summe der hypergeometrischen Zufallsvariablen beschrieben. Es folgt

$$p_E = \sum_{n_Z=n_T}^{n_A} \binom{n_G \cdot p_A}{n_Z} \cdot \binom{n_G - (n_G \cdot p_A)}{n_G - n_Z} \cdot \binom{n_G}{n_A}^{-1}$$

Ist die Anzahl n_A der Peers, an die eine Anfrage gesendet wurde gering im Vergleich zur Anzahl n_G der Peers im P2P System, kann die hypergeometrische durch eine binomische Zufallsvariable abgeschätzt werden. Insgesamt kann p_E sowohl für den vollständigen und den eingeschränkten Broadcast als auch für die koordinierte Strategie durch eine Summe binomischer Zufallsvariablen beschrieben werden. Es folgt

$$p_E = \sum_{n_Z=n_T}^{n_A} \binom{n_A}{n_Z} \cdot p_A^{n_Z} \cdot (1-p_A)^{n_A - n_Z}$$

Abbildung 2 zeigt den Verlauf der Erfolgswahrscheinlichkeit bzgl. der Parameter n_A und n_T für eine Antwortwahrscheinlichkeit $p_A=0.9$. Intuitiv wächst p_E mit steigender Anzahl n_A versendeter Anfragen bzw. mit fallender Anzahl n_T benötigter Antworten.

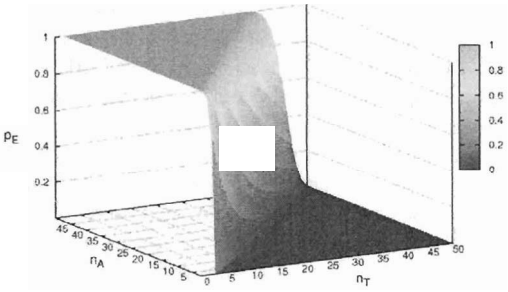


Abb. 2: Verlauf der Erfolgswahrscheinlichkeit bzgl. n_A und n_T

Eine geschlossene Form der Erfolgswahrscheinlichkeit p_E kann mit Hilfe der Chernoff-Ungleichung berechnet werden. Es gilt

$$p_E \geq \frac{p_A \cdot (n_A - n_T + 1)^{n_T - 1}}{(1-p_A) \cdot (n_T - 1)} \cdot \left(\frac{(1-p_A) \cdot (n_T - 1)}{n_A - n_T + 1} + (1-p_A) \right)^{n_A}$$

Mit dieser Formel kann z.B. n_A bzgl. eines gewünschten p_E eingestellt werden.

V. Literaturverzeichnis

[1] Kanchanasut, K. et al.: A Multimedia Communication System for Collaborative Emergency Response Operation in Disaster-affected Areas; Internet Education and Research Laboratory (intERLab), Asian Institute of Technology (AIT), 2007

[2] HiMoNN - an efficient and highly mobile Ad-hoc Network Node; http://www.iabg.de/infokom/fachthemen/himonn_en.php

[3] Neuman, C.; Yu, T.; Hartman, S. & Raeburn, K.: The Kerberos Network Authentication Service (V5); IETF RFC 4120, 2005

[4] Shamir, A.: How to Share a Secret; Communications of the ACM, 1979, 22, 612-613

[5] Shoup, V.: Practical Threshold Signatures; Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRPYT 2000), Springer, 2000, 1807, 207-220

[6] Boldyreva, A.: Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme; Proceedings of the 6th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003), Springer, 2003, 2567, 31-46

[7] Saxena, N.; Tsudik, G. & Yi, J. H.: Admission Control in Peer-to-Peer: Design and Performance Evaluation; Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), ACM Press, 2003, 104-113