ulm university universität
uulm

WMAN 2008 - KuVS Fachgespräch über Mobile Ad-hoc Netzwerke

Matthias Frank, Frank Kargl, Burkhard Stiller (Hg.)

Ulmer Informatik-Berichte

Nr. 2008-06
April 2008

WMAN 2008
KuVS Fachgespräch über Mobile Ad-hoc Netzwerke

Bereits zum fünften Mal treffen sich dieses Jahr Forscher aus Deutschland und den europäischen Nachbarländern, um unter dem Dach des "Workshop on Mobile Ad-hoc Networks" Erfahrungen und Forschungsergebnisse auszutauschen und neue Ideen zu diskutieren.

Nachdem der WMAN 2002 als eigenständige Veranstaltung abgehalten wurde, folgten 2004 und 2005 Veranstaltungen unter dem Dach der GI Jahrestagungen in Ulm und Bonn. 2007 fand der WMAN Workshop dann als Workshop der Konferenz "Kommunikation in Verteilten Systemen (KiVS) 2007" in Bern statt.

Für 2009 ist wieder geplant, einen KiVS- Workshop anzubieten. Um die Kontakte und Diskussionen in diesen zwei Jahren nicht abreißen zu lassen, bieten wir 2008 nun ein neues Format an: ein WMAN Fachgespräch. In der Ausrichtung und den Anforderungen an die Beiträge ist dieses deutlicher flexibler als ein vollständiger Workshop. Primäres Ziel ist ein informeller Gedankenaustausch, der durch Vorträge und kurze Beiträge unterstützt wird, die in Form dieses technischen Berichtes veröffentlicht werden.

Themen der diesjährigen Beiträge sind verschiedenste Aspekte mobiler Ad-hoc Netzwerke, angefangen von der Nutzung von VoIP in Mesh Netzen, Beiträgen zu taktischen Ad-hoc Netzwerken und VANETs bis hin zur Tool-Unterstützung.

Die Beiträge im Einzelnen:

Bei diesen interessanten Themen wünschen wir allen Teilnehmern ein spannendes und diskussionsreiches Fachgespräch.

Ulm, den 24. April 2008

Matthias Frank, Frank Kargl, Burkhard Stiller

Adaptive Aggregierung von VoIP Paketen in Wireless Mesh Networks

Peter Dely, Andreas J. Kassler
Karlstads Universitet, Universitetsgatan 2, SE-65188 Karlstad, Schweden
peter.dely@kau.se; kassler@ieee.org

I. Einleitung

Voice over IP (VoIP) gewinnt auch in drahtlosen Netzwerken zunehmend an Popularität. Aufgrund des 802.11 MAC Layers entsteht beim Transfer von VoIP-Paketen über drahtlos LAN (WLAN) ein großer Overhead. Die Übertragung eines G.729 VoIP Rahmens inklusive der nötigen RTP/UDP/IP Header auf einem IEEE 802.11a Link mit 24 MBit/s nimmt dabei ca. 20 µs in Anspruch. Overhead des 802.11 DCF MAC Protokolls (wie SIFS, DIFS, ACK, Back-off) und PHY-Overhead (Preamble, PLCP Header) hingegen belegen den Kanal für ca. 46 µs. Dies ist mit ein Grund für die niedrige VoIP Kapazität von WLANs. Das Problem verstärkt sich in Wireless Mesh Networks (WMNs), da Access Points miteinander drahtlos kommunizieren und so ein vermaschtes drahtloses Netz bilden. In diesem multi-hop Scenario fällt die Kapazität etwa entsprechend $1/n$ (n=Anzahl Hops) [1], wenn nicht multi-channel Lösungen verwendet werden.

Um die Kapazität zu erhöhen, schlagen etwa [1], [2] und [3] vor, mehrere kleine VoIP-Pakete zu einem großen Packet zu aggregieren, mit einem zusätzlichen IP-Header zu versehen und auf einmal zu senden. IEEE 802.11n beinhaltet einen ähnlichen Mechanismus auf MAC-Schicht. Paketaggregierung reduziert dabei den Overhead. Da weniger Pakete gesendet werden und der Kanal somit weniger benutzt wird, verringert sich auch die Kollisionswahrscheinlichkeit. Als Konsequenz steigt die VoIP Kapazität des Netzwerkes. Bei der Aggregierung von VoIP Paketen sind allerdings einige Einschränkungen zu beachten. Um genügend Pakete aggregieren zu können, müssen diese verzögert und gepuffert werden. Da die maximale End-zu-End Verzögerung kritisch für die Qualität von VoIP Verbindungen ist, dürfen Pakete nicht zu lange verzögert werden. Werden die Pakete zu kurz verzögert, können nur wenige Pakete aggregiert werden und die Verringerung des Overheads ist gering. Eine weitere Einschränkung sind Bitfehler im Übertragungskanal. Bei einem konstanten Signal-Rauschabstand (SNR) haben längere Pakete eine höhere Fehlerwahrscheinlichkeit als kurze [4]. Ist die Fehlerwahrscheinlichkeit zu hoch, kommt es zu Neu-Übertragungen auf dem MAC-Layer und schlussendlich auch zu Ende-zu-Ende Paketverlust und zusätzlicher Verzögerung.

Es lassen sich zwei Ansätze zur Aggregierung unterscheiden. Bei der End-to-End Aggregierung, aggregiert nur der Sender bzw. der Ingress-Mesh-Router [3]. Im Gegensatz dazu werden bei der zweiten Variante, der Hop-by-Hop Aggregierung, Pakete auf jedem Mesh Router aggregiert bzw. Deaggregiert [1]. Während sich die End-to-End Aggregierung vor allem durch eine einfache Implementierung auszeichnet, bietet die Hop-by-Hop Aggregierung mehr Flexibilität. Es gibt mehr Aggregierungsmöglichkeiten, da alle Pakete mit dem gleichen nächsten Hop und nicht nur Pakete mit gleicher Empfängeradresse zusammengefasst werden können. Außerdem erlaubt die Hop-by-Hop Aggregierung längere Pakete auf Links mit guter Signalqualität und kürzere Pakete auf schlechten Links zu senden. In WMNs sollte daher, im Gegensatz zu [3], die optimale Paketgröße daher für jeden Hop und nicht für die gesamte Route festgelegt werden.

II. Lösungsansatz

Zur Leistungssteigerung von VoIP in WMNs schlagen wir einen Hop-by-Hop Aggregierungsalgorithmus vor. Der Algorithmus legt die maximale Paketgröße abhängig von der Linkqualität fest. Dadurch ist die maximale Paketgröße nicht durch den schwächsten Link einer Route limitiert. Mit Hilfe von Simulationen zeigen wir, dass die adaptive Bestimmung der maximalen Paketgröße zu einer signifikanten Performancesteigerung führt.

Bei unserem Ansatz werden die Pakete in einem Ausgangspuffer, welcher sich vor dem MAC-Layer befindet, aggregiert, indem die zu aggregierenden VoIP-Pakete in ein neues IP-Paket eingepackt werden. Sollte der MAC-Layer gerade belegt sein, entsteht eine Verzögerung, welche bei geringer Netzlast allerdings zu klein ist um genügend Pakete zur Aggregierung zu sammeln. Daher werden die Pakete zusätzlich künstlich verzögert. Der Algorithmus wird durch die drei Variablen $SIZE_{min}$, MAX_{delay} und $SIZE_{max}$ gesteuert, wobei der Netzwerkbetreiber die ersten beiden statisch festsetzten kann. Der Aggregierungspuffer verzögert das Paket bis mindestens $SIZE_{min}$ Bytes vorhanden sind. Sind weniger als $SIZE_{min}$ Bytes vorhanden und das älteste Paket P_0 verweilt länger als MAX_{delay}, dann werden die Pakete mit gleichem nächsten Hop wie P_0 aggregiert und gesendet. Durch $SIZE_{min}$ und MAX_{delay} wird sichergestellt, dass auch bei mittlerer Netzlast Pakete aggregiert werden, bei geringer Netzlast die

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS, which receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

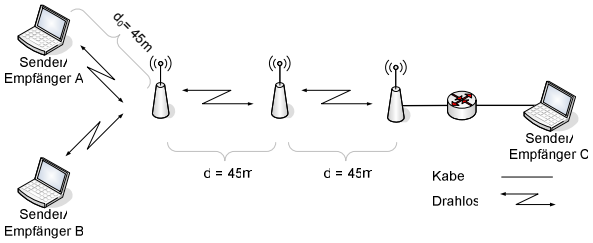

Abbildung 1. Simulationstopologie.

Verweildauer in der Warteschlange jedoch nicht zu lange ist. Die maximale Paketgröße $SIZE_{max}$, d.h. wie viele VoIP Pakete maximal zusammengefasst werden, wird durch einen verteilten Algorithmus bestimmt. Zuerst bestimmt der Empfänger (next hop) fortlaufend die SNR aller empfangen Pakete (getrennt nach Sender) und speichert den gleitenden Durchschnitt. Diese Information fügt er Routing-Nachrichten hinzu (z.B. AODV-HELLO), welche periodisch an alle Nachbarn versendet werden. Somit erfährt der Sender die SNR für jeden Link. Die SNR am Empfänger zu messen ist notwendig, weil asymmetrische Links in Richtung A-B eine andere Qualität als in Richtung B-A haben.

Für eine gegebene SNR und Signalkodierung ist die theoretische Bitfehlerwahrscheinlichkeit (BER) bekannt. Eine obere Schranke für die Framefehlerwahrscheinlichkeit (FER_{MAX}) ist lässt sich aus [4] bestimmen, wobei der Modulationsmodus sowie der Einfluss des Faltungscoders berücksichtigt werden muss. Der Sender kann somit jene Framelänge bestimmen, welche FER_{MAX} nicht übersteigt. Da die meisten VoIP-Codecs eine geringe Anzahl an fehlenden Paketen ohne merkbaren Qualitätsverlust ausgleichen können, kann die maximale Paketgröße so gewählt werden, dass die FER größer als 0% ist (etwa 0,1%). Der Sender setzt $SIZE_{max}$ für jeden Link so fest, dass diese Framefehlerwahrscheinlichkeit nicht überschritten wird.

III. Leistungsbewertung

Die Leistung des Algorithmus haben wir im populären Netzwerksimulator ns-2 (Version 2.26) [5] evaluiert. Die verwendete Topologie ist in Abbildung 1 dargestellt. Bei einem Abstand von 45 m ist die Signalqualität exzellent, es treten praktischen keine Bitfehler auf. Bei 85 m ist die Bitfehlerwahrscheinlichkeit nahe 100%. Der ns-2 MAC/PHY-Layer wurde erweitert, sodass Bitfehler und Framefehler gemäß [4] auftreten. Wir verwenden 802.11a mit 6 Mbps Basisrate und 24 Mbps Datenrate, MAX_{delay} wurde auf 10 ms und $SIZE_{min}$ auf 300 bytes gesetzt. Der VoIP Verkehr wurde mittels der VoIP-Erweiterung aus [6] erzeugt, welche es erlaubt, den Mean Opinion Score (MOS) eines VoIP-Datenstromes zu bestimmen. Die Sender/Empfängerpaare sind Nodes A-C, C-A, B-C und C-B. Die Aggregierung findet nur auf den drahtlosen Links statt.

Als Leistungsmetrik verwenden wir die VoIP-Kapazität des Netzwerkes. Wir legen die VoIP-Kapazität als die maximale Anzahl der parallelen VoIP-Einwegdatenströme fest, sodass 95% der Datenströme eine MOS größer als 3,5 (entspricht akzeptabler Qualität) haben. Die Evaluierung vergleicht drei Verfahren: keine Aggregierung, Aggregierung mit statischem $SIZE_{max}$ (2300 Bytes) und mit adaptiven $SIZE_{max}$.

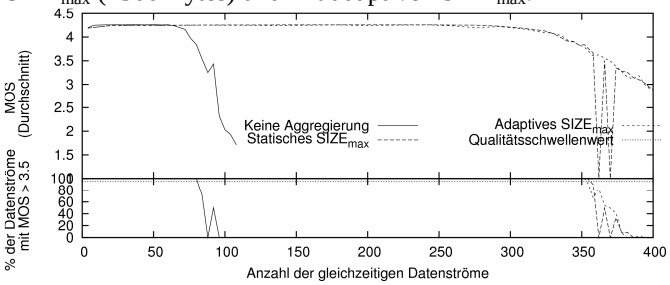

Abbildung 2. Durchschnittliche MOS mit d_0=d_1=45 m.

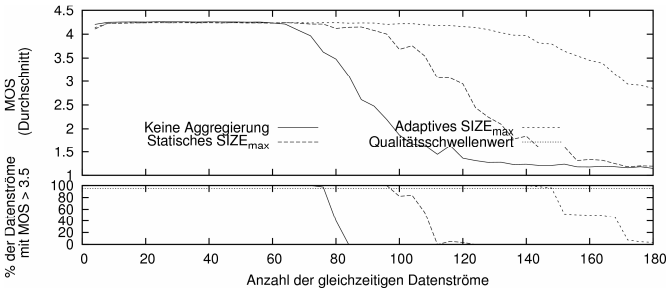

Abbildung 3. Durchschnittliche MOS mit d_0=77 m, d_1=45 m.

Abbildung 2 zeigt die mittlere MOS und den Prozentsatz der Datenströme mit einer MOS größer als 3,5 dargestellt. Wenn keine Aggregierung benutzt wird, bleibt die MOS für bis zu 80 gleichzeitige Datenströme konstant bei ca. 4,2. Danach kommt es zu Kollisionen und Retransmissions. Schließlich kann der MAC-Layer den neu ankommenden Verkehr nicht mehr bewältigen und die Puffer laufen über. Wird jedoch Aggregierung verwendet verschiebt sich dieses Kapazitätslimit durch die Overheadreduktion auf 354 gleichzeitige Datenströme. Die Kapazität wird also mehr als vervierfacht. In Abbildung 3 wurde die Distanz d_0 von 45 auf 77 Meter erhöht. Dadurch verschlechtert sich die Signalqualität und FER für zu lange Pakete steigt rapide an. Bei einem statischen $SIZE_{max}$ können die zu langen Pakete zu Framefehlern führen. Die Kapazität mit statischem $SIZE_{max}$ beträgt 96 gleichzeitige Datenströme. Wird $SIZE_{max}$ jedoch adaptiv begrenzt, so treten auf dem schlechten Link sehr wenige Framefehler auf und die Kapazität steigt auf 148. Das bestätigt, dass die maximale Paketlänge abhängig von der Linkqualität gewählt werden sollte.

Referenzen

[1] K. Kyungtae and H. Sangjin, "VoMESH: voice over wireless mesh networks," *in Proc. of IEEE WCNC*, Las Vegas, USA, 2006, pp. 193-8.

[2] S. Ganguly et al., "Performance Optimizations for Deploying VoIP Services in Mesh Networks", in *IEEE JSAC*, 2006. p. 2147-2158.

[3] R. Raghavendra, A. P. Jardosh, E. M. Belding, and H. Zheng, "IPAC – An IP-based Adaptive Packet Concatenation for Multihop Wireless Networks," in *Proc. of Asilomar Conference on Systems, Signals and Computing*, Pacific Grove, CA, 2006.

[4] S. Mangold. S. Choi and N. Esseling, "An Error Model for Radio Transmissions of Wireless LANs at 5GHz", in Proc. of 10th Aachen Symposium on Signal Theory, Aachen Germany, 20-21.9 2001.

[5] The Network Simulator - ns-2, Available: http://nsnam.isi.edu/nsnam/index.php/Main_Page

[6] A. Bacioccola, C. Cicconetti and G. Stea, "User level performance evaluation of VoIP using ns-2", in *Proc. of First International Workshop on Network Simulation Tools*, Nantes (FR), Oct. 22, 2007.

LHA Protocol: Powerful Solution for Merging and Partitioning Ad hoc Networks

Ausama Yousef and Andreas Mitschele-Thiel
Integrated HW/SW Systems Group
Ilmenau University of Technology
98693 Ilmenau, Germany
Email: ausama.yousef, mitsch@tu-ilmenau.de

***Abstract*—Address auto-configuration process is one of the most essential issues for Ad hoc networks (MANETs). Before nodes participate in multi-hops communication, they must be assigned an IP address. Uniqueness, fast assignment, conflicts solving and reusability of the IP addresses in MANETs are the main topics of the auto-configuration process. Several address auto-configuration protocols have been proposed for MANETs. However, in case of failures due to partitioning and merging networks, these protocols fail to satisfy all of those topics. In this work we present a new proposal to handle the MANETs issues in case of partitioning and merging networks.**

I. Introduction

There are several limitations of already proposed auto-configuration protocols designed for Ad hoc networks as in [1] and [2]. They suffer from low efficiency which is caused by large protocol overhead, resources limitations and potential address conflicts during partitioning and merging operations.

The Logical Hierarchical Addressing (LHA) protocol [3] is proposed as a novel auto-configuration protocol for distributed addressing and handling the related issues in MANETs. The LHA protocol provides a fast mechanism to configure a joining node with a unique address. Depending on an equation the address of the new node is calculated by one of its neighbours which have already connected to the network.

II. LHA Basic Idea

For simplicity, the following block 192.168.0.0 - 192.168.255.255 (192.168/16 prefix) of private IPv4 addresses is used in our solution for addressing the hosts within a MANET. However the LHA protocol is applicable for each block of private IPv4 addresses or IPv6 addresses. As is generally known, the used block consists of two parts, MANET ID and host ID as shown in figure1.

MANET ID 16bit (192.168)	Host ID 16bit

Fig. 1. Use of private IPv4 addresses

We treat the available 16-bit block of IP addresses as a set of disjoint sub blocks. Every node manages one of the sub blocks of free addresses. Any node can act as an Address Agent (AA) and assigns one of its free addresses to a requester node. A requester node chooses its AA node from its neighbors. In our approach there are two additional roles for a node in the network, predecessor and successor. The AA node, which provides an address to the requester is called predecessor for the requester node. Analogously, the requester is called the successor of its AA node. Every predecessor can have K direct successors, whereas every node has only one predecessor. In this way a logical address hierarchy is built in the network. The first node in this hierarchy is called the Root and it does not have any predecessor. Every node maintains a table containing information about addresses and parameters of its successors and its predecessor called hierarchy table.

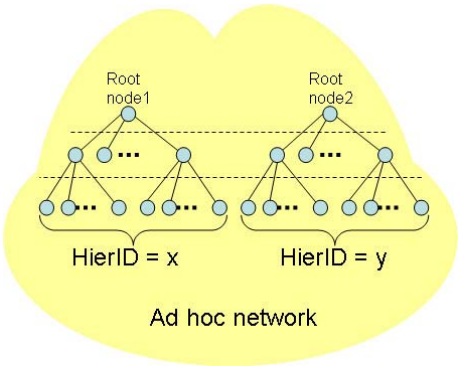

Fig. 2. Possible structure of address hierarchy in an Ad hoc network

Our protocol makes it possible to build more than one address hierarchy in each Ad hoc network as shown in figure 2. Our proposal to do that is to divide logically the Host ID in two parts: Hierarchy ID (HierID, 6 bits) and Hierarchical Host ID (HHID, 10 bits) as depicted in figure 3.

MANET ID 16bit (192.168)	HierID 6bit	HHID 10bit

Fig. 3. Division of private IPv4 addresses block in LHA protocol

The number of bits in each part is calculated as follows: HHID = floor (2*available bits block/3) and HierID = available bits block - HHID. The selection of this division based on the comparison of the occurrence rat of merging and partitioning networks with the same rate of assigning addresses.

According to our algorithm in figure 2 each root node chooses randomly its HierID. Then each node belonging to one of those roots uses the same HierID of its root in its

IP address, and thus more than one address hierarchy can be build in an Ad hoc network. Advantages of this proposal can be noticed later in case of partitioning and merging networks.

III. PARTITIONING AND MERGING NETWORKS

A. Network Partitioning

The LHA algorithm solves the problems of partitioning and merging of networks. In case of a partitioning, the nodes continue to assign unique addresses as shown in figure 4. Subsequently, if the two parts merge again, there are no duplicated addresses because the nodes in each of the two parts have assigned disjunct addresses. This is due to the application of the conditions and equations described in [3]. If the AA node in one partition fails to assign an available address to the requester it should check the parameter of the total number of lost nodes $n_{lost-node}$. In the case that $n_{lost-node} >$ threshold, the AA node detects the network partitioning. If this happens there are two cases depending on the existence of a root node.

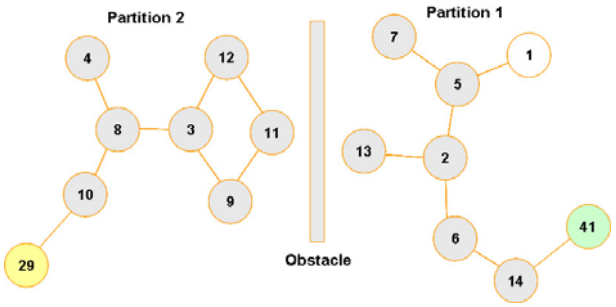

Fig. 4. New nodes get their addresses, which are unique in each part, from the AA nodes (node 10 and 14 are AA nodes for new node 29 and 41 respectively)

In the case there is a root node in the partition, the node detecting the partitioning increases HierID by 1. Then it floods Inc-HierID messages to all nodes. Upon receiving this message the nodes increment their HierID as well. Then they change the missing addresses of their successor into available addresses. After that the network works such as described in the algorithm in [3]. In case there is no root node, the AA node decreases the HierID by 1 and assigns the address of the root node to the new node. After that, the new node floods Dec-HierID messages including the decremented HierID and a new NetID to all the nodes. Upon receiving this message, the nodes execute the required changes. Then they change the missing addresses of their successors into available addresses which can be used again. After that, the network continues with regular operation. From this discussion we can see that the partitioning problem is solved using our solution even if the two partitions merge again.

B. Network merger

As discussed above, the merging of two partitions previously formed from one network cannot cause duplicated addresses. However, when two different networks (e.g. A and B) merge as depicted in figure 5, there is a probability of

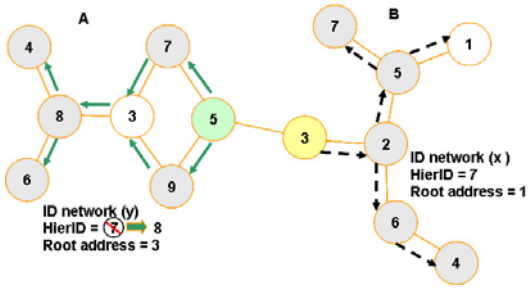

Fig. 5. Merging of two networks having the same HierID

duplicated addresses, i.e. if the HierIDs are the same in the both networks.

In our proposal every node in each network sends beacon messages which include its IP address and the NetID. Upon receipt of this message any node can detect the merging of two networks. There are two kinds of merging, soft and hard: The soft merging can not cause any duplicated addresses due to the difference of the HierIDs in the two networks. In this case the responsible node detecting the merging broadcasts a Soft Merging message (S-Mer) to the other nodes. This message includes the HierID and NetID of another network. The other nodes save this information in their table. Later in next merging, any node can detect the merging and can decide the kind of merging.

If the HierIDs are the same in the two networks as shown in figure 5, the node detects a hard merging. Here the probabilities of duplicated addresses are high. The node can solve this problem by comparing its root address with the received one. In case of different root addresses the node with the larger root address saves the NetID of the other network. Then it broadcasts hard merging messages (H-Mer) to all the nodes in the network. Every node which belongs to the sender's network has to increment its HierID by 2 and save the two values (HierID and NetID) of the other network. If the root addresses are the same, the detecting node compares the NetIDs. Then the node with the larger NetID will send H-Mer messages. Thus, possible address conflicts in the network are solved.

IV. CONCLUSION

Our LHA protocol enables MANET nodes to be configured with an address very rapidly upon joining a network. We have proposed a new solution to the partitioning and merging networks. This solution depends on LHA algorithm for building the multi-logical address hierarchy in the network.

REFERENCES

[1] S. Kim, J. Lee and I. Yeom "Modeling and Performance Analysis of Address Allocation Schemes for Mobile Ad Hoc Networks," *in IEEE Transactions on Vehicular Technology . 57(1)*,2008, pp. 490-501.

[2] Y. S. Chen, T. H. Lin and S. M. Lin." RAA: a ring-based address autoconfiguration protocol in mobile ad hoc networks," *Wireless Pers Commun, Springer Netherlands, 43(2)* ,2007, pp. 549-571.

[3] A. Yousef, H. Al-Mahdi, M. Abd rabou Kalil and A. Mitschele-Thiel, "LHA: Logical Hierarchical Addressing Protocol for Mobile Ad hoc Networks," in *10th ACM/IEEE Int. Symp.(MSWiM 2007)*, Chania, Crete Island, Greece, October, 2007, pp. 96-99.

Offline Time Synchronization for libpcap Logs

Daniel Marks, Wolfgang Kiess, Björn Scheuermann, Magnus Roos, Martin Mauve, and Florian Jarre

Heinrich Heine University, Düsseldorf, Germany

I. Introduction

A fundamental problem in real-world computer network experiments is that each system uses its own local clock to timestamp events. These clocks are not perfectly accurate, and thus deviate from each other. Event timestamps assigned by different nodes can therefore not immediately be compared, making the analysis of experimental results difficult. The synchronization of the clocks *online* during the experiment is at most a partial solution to the problem. While using high-precision, special-purpose clocks implies high effort and expensive hardware, online time synchronization protocols like NTP [3] require a permanent, reliable network connection between each node and a reference clock. This cannot always be guaranteed during an experiment. Using such a time synchronization protocol also generates network traffic, which might interfere with the traffic of the experiment itself, and therefore potentially influences the results. Furthermore, even if the clocks were perfectly synchronized, it takes some system dependent (and potentially non-deterministic) time from the occurrence of an event until it is actually timestamped and recorded. While it may be possible to use customized hard- and software to bound this delay, such a solution cannot be employed for the off-the-shelf systems often used in network experiments.

In order to avoid these problems we have proposed in earlier work [4] to record the occurring events with the deviating, local clocks and synchronize the resulting event log files offline after the experiment. The synchronization is based on so-called *anchor points*, that is, on events that have been recorded and timestamped by more than one node in parallel. The anchor points allow to set the clocks of the nodes into relation. In networks where the medium has a broadcast characteristic (like many wireless networks, but also Ethernet using hubs), the (almost) parallel reception of a packet transmission by multiple nodes can serve as such an anchor point.

In [4], we laid the foundations of this technique. Here, we go one step further and discuss aspects that arise if it is to be applied in a real network. We introduce `pcapsync`, a tool using the algorithm from [4] to synchronize event logs from experiments in IEEE 802.11 wireless networks. It reads a set of log files that have been recorded in libpcap format (used, e. g., by tcpdump [5] and Wireshark [6]), identifies potential anchor points in them, applies our offline time synchronization algorithm, maps the recorded local timestamps to a common, global time scale, and finally writes back a corresponding set of synchronized libpcap files. Its output can thus immediately be used for further analysis with standard tools.

II. MLE Time Synchronization

The synchronization algorithm used by `pcapsync` has been introduced in [4], here we provide a rough overview. As its input, the algorithm is given a set of events that have each been observed by two or more nodes (i. e., the anchor points), and their local timestamps. These events provide information about multiple nodes' clocks at a common point in time. The output includes estimates for the clock rates and offsets, and a synchronized timestamp for each of the anchor points.

The approach assumes clocks to be linear, which is a good approximation at least for experiment durations of up to about 20 minutes. Clocks are thus characterized by a *rate* r and an *offset* o. When read at "true" time[1] T, the clock shows

$$C(T) = r \cdot T + o. \tag{1}$$

Based on additional assumptions on the timestamping process, a maximum likelihood estimator (MLE) for rates, offsets, and event times can be established. This reduces the synchronization problem to an optimization problem. By substitutions and transformations, the MLE can be expressed as a linear program (LP). However, with an increasing number of nodes and anchor points the matrix of coefficients of the LP soon becomes very big, so that standard LP solvers cannot be applied in a straightforward way.

The matrix is very sparse, though. It can be arranged in a special way such that its structure can be exploited to reduce both computational and storage complexity. We use an interior point method, a variant of Mehrotra's predictor-corrector algorithm [2], to solve the linear program. Analytical, simulative, and experimental evaluations presented in [4] show that the estimate is good even for a relatively limited number of available anchor points, and quickly improves further as their number increases.

III. Pcapsync

To apply MLE timestamp synchronization to real-world experiments in IEEE 802.11 networks, we have implemented the `pcapsync` tool. Figure 1 gives an overview of `pcapsync`'s general operation. In its initial step, it parses sets of libpcap log files and identifies anchor points. Anchor points are the foundation of MLE synchronization, and its performance crucially depends on correctly identifying them. In `pcapsync`, we use parallel receptions of the same transmission as anchor points. For a real wireless network, it is thus necessary to identify groups of timestamped packet receptions in the libpcap files,

[1] An absolute time scale does of course not exist; it is, however, assumed here for simplicity.

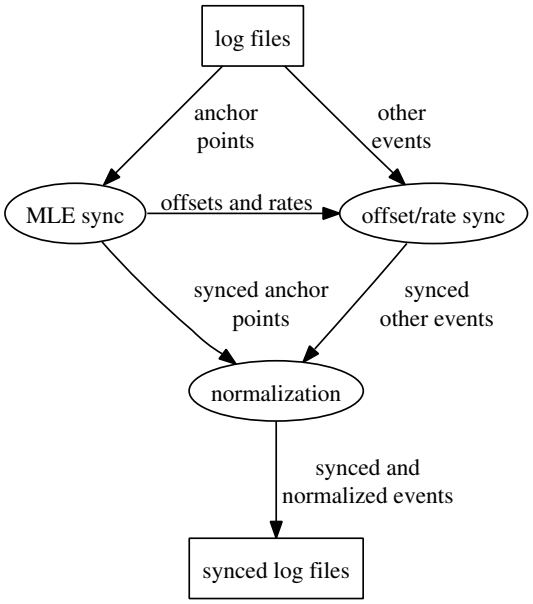

Fig. 1. Structure of pcapsync.

from which it is known for sure that they belong to the same physical transmission. One central duty of `pcapsync` is thus to identify such events.

The link layer reliability mechanism in IEEE 802.11 retransmits unicast packets up to seven times if an acknowledgment is missing [1]. If multiple nodes receive the same unicast transmission[2], these events therefore do not necessarily belong to the same physical layer transmission: for example, as shown in Figure 2, it may well happen that one node receives only the first transmission attempt, while another node receives only the second one. Unfortunately, it is not possible to record the number of performed retransmissions in a hardware-independent way. A packet reception log entry also does not reveal which (re)transmission attempt has been received. Thus, in the specific case of 802.11, multiple receptions of the same unicast packet cannot be used as anchor points.

For broadcast packets there is no automatic retransmission. Still, however, it can happen that identical broadcast packets recorded in the log files refer to different transmissions since higher layers may generate multiple copies of the same packet. ARP, for instance, often broadcasts identical requests when the same address is resolved again. However, broadcast packets generated multiple times can easily be identified using the records about sent packets in the log files. Consequently, they are not used as anchor points. In summary, `pcapsync` is able to use parallel receptions of globally unique broadcast transmissions as anchor points for the synchronization in 802.11 networks.

Based on these rules, the events that can be used as anchor points and those which are not suitable for this purpose can be identified and separated. For the anchor points, synchronized

[2]Note that this is generally possible if the log files are recorded in promiscuous mode.

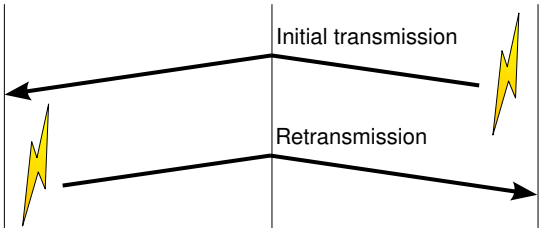

Fig. 2. Ambiguous reception times in case of retransmissions.

timestamps are estimated by the MLE algorithm. As it also yields estimates for clock rates and offsets of all nodes, the timestamps of all other events can be corrected by applying a linear transformation. For an event observed at local time t by some node with estimated clock rate $\widehat{r}$ and estimated offset $\widehat{o}$, it can easily be seen from (1) that the corrected, global timestamp $\widehat{T}$ is given by

$$\widehat{T} = \frac{t - \widehat{o}}{\widehat{r}}. \tag{2}$$

After calculating global timestamps for all events, `pcapsync` normalizes them such that the first event in the experiment occurs at time zero. For this normalization, the globally earliest synchronized event timestamp is subtracted from all timestamps.

Finally, `pcapsync` writes the data to new, synchronized per-node log files. To simplify the evaluation and visualization of an network experiment, it also offers the option to write the synchronized data into one global log file.

IV. Conclusion

In this paper, we have introduced `pcapsync`, a tool for the offline time synchronization of libpcap log files recorded in experiments with IEEE 802.11 networks. This tool is based on MLE timestamp synchronization [4], which uses parallel event observations to relate the clocks of different nodes. We have discussed how suitable events can be identified in real world log data. We have also shown how globally synchronized timestamps can be obtained also for other events. In summary, we believe that `pcapsync` will prove a valuable tool for evaluating experimental results.

Acknowledgments

Part of the work presented here has been supported by the German Research Foundation (DFG).

References

[1] IEEE LAN MAN Standards Committee. ANSI/IEEE Std 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
[2] S. Mehrotra. On the implementation of a primal-dual interior point method. *SIAM Journal on Optimization*, 2(4):575–601, 1992.
[3] D. Mills. Network Time Protocol (Version 3) Specification, Implementation and Analysis. RFC 1305 (Draft Standard), Mar. 1992.
[4] B. Scheuermann, W. Kiess, M. Roos, F. Jarre, and M. Mauve. On the time synchronization of distributed log files in networks with local broadcast media. *IEEE/ACM Transactions on Networking*. In press.
[5] tcpdump: a tool for network monitoring, protocol debugging and data acquisition. http://www.tcpdump.org.
[6] The wireshark network protocol analyzer. http://www.wireshark.org/.

Aktuelle Trends in der sicheren Fahrzeug-Fahrzeug Kommunikation

Frank Kargl, Elmar Schoch, Zhendong Ma
Universität Ulm, Institut für Medieninformatik
{*vorname.nachname*}@uni-ulm.de

***Zusammenfassung*—Dieser Beitrag zeigt aktuelle Trends der Informationsverteilung in Fahrzeug-Fahrzeug Netzen und analysiert Auswirkungen auf und mögliche Lösungsansätze für Sicherheit und Schutz der Privatsphäre.**

I. Einleitung

Seit einigen Jahren wird das Thema der Fahrzeug-Fahrzeug-Kommunikation vor allem in den USA, in Europa und in Japan intensiv untersucht. Ausgehend von initialen Forschungsprojekten der ersten Generation wie Fleetnet oder VSC wurden einerseits weitere Forschungsaktivitäten gestartet (z.B. Network-on-Wheels, VII, CVIS, Safespot), andererseits arbeiten verschiedene Organisationen bereits an der Standardisierung von Kommunikationsmechanismen und Protokollen. Hier sind vor allem die Aktivitäten der IEEE (802.11p, 1609.x), ISO-CALM und das Car-2-Car Communication Consortium zu nennen.

Im Rahmen dieser Aktivitäten wird bereits die Sicherheit und der Datenschutz zukünftiger Systeme untersucht. In den USA mündete dies in den vorläufigen IEEE 1609.2 Standard, in Europa ist in diesem Bereich vor allem das Projekt Secure Vehicle Communication (SeVeCom) aktiv.

All diesen Standardisierungsbemühungen und Projekten ist zu eigen, dass sie eine relativ abgegrenzte Menge von Kommunikationsformen betrachten. Dies sind vor allem

1) **Beaconing:** direktes und periodisches Senden von Broadcast-Nachrichten an alle Nachbarn in Reichweite der drahtlosen Kommunikationstechnologie.
2) **Flooding und Geocast:** Verteilung[1] von Broadcast Nachrichten, wobei Empfängerknoten Nachrichten auch weiterleiten. Um die Weiterleitung zu begrenzen, kommen z.B. Time-to-Life (TTL) Zähler oder im Falle von Geocast [1] die Angabe eines geographischen Verbreitungsgebiets zum Einsatz.
3) **Positionsbasiertes Routing:** Im Gegensatz zu topologie-basiertem Routing, wie es oft in MANETs eingesetzt wird, hat sich bei Fahrzeug-Fahrzeug Netzen positionsbasiertes Routing als besser geeignet erwiesen [2].

Dies sind auch die Mechanismen, deren Sicherheits- und Datenschutzaspekte am genauesten untersucht wurden (z.B. in [3], [4]). In jüngerer Zeit gibt es jedoch Hinweise und Aktivitäten, die darauf hindeuten, dass diese einfachen Kommunikationsformen manche Anwendungen nicht ausreichend unterstützten.

Deshalb werden aktuell zusätzliche Kommunikationsverfahren untersucht, welche im folgenden Abschnitt kurz vorgestellt werden sollen. Anschließend wird diskutiert, inwiefern diese anderen Formen der Kommunikation auch geänderte Anforderungen an ein Sicherheitssystem stellen.

[1] gegebenenfalls auch periodisch

II. Fortgeschrittene Kommunikationsmuster

Ein Ansatz, der in jüngerer Zeit untersucht wird, ist die *Effizienzsteigerung bei Flooding und Geocast*. Abhängig von Netzwerkparametern wie Knotendichte oder Topologie muss gegebenenfalls nicht jeder Knoten ein empfangenes Packet erneuten broadcasten. Statt dessen verwenden die verschiedenen Varianten des sog. Gossiping [5] eine geringere Weiterleitungswahrscheinlichkeit, die entweder statisch oder anhand von Netzwerkparametern festgelegt wird. Damit lassen sich signifikante Effizienzsteigerungen erzielen.

Bei der *Context-adaptive Message Dissemination* [6] geht es ebenfalls um das Verteilen von Paketen bzw. Informationen. Hier speichert jeder Empfänger von Daten diese zunächst lokal und entscheidet dann anhand einer Relevanzfunktion, welche Daten er im momentanen Kontext für besonders wichtig für seine Nachbarn hält und schickt diese priorisiert weiter. Parameter können Abstand zum Ursprung der Information, deren Alter, uvm. sein. Durch eine Anpassung der Wartezeiten im Medienzugriff kann darüber hinaus auch eine Priorisierung zwischen Knoten erreicht werden. *Context-adaptive Message Dissemination* sorgt vor allem dafür, dass bei einer gegebenen Netzwerkkapazität diese vor allem zur Weiterleitung der relevanten Informationen genutzt wird.

Aggregation geht noch einen Schritt weiter. Hier empfängt ein Fahrzeug Daten von seinen Nachbarn, z.B. über deren aktuelle Geschwindigkeit. Vor einer möglichen Weiterleitung werden diese Daten allerdings zunächst aggregiert, d.h. zusammengefasst. Dies kann sinnvoll sein, wenn z.B. bei einem Stau sehr viele Fahrzeuge gleiche oder ähnliche Informationen senden. Hier wird also die Menge der zu sendenden Information direkt reduziert und damit die Kommunikationslast reduziert.

III. Sicherheit bei fortgeschrittenen Kommunikationsmustern

Betrachtet man Gossipping, Context-adaptive Message Dissemination und Aggregation unter dem Aspekt von Sicherheit und Schutz der Privatsphäre, so stellt man fest, dass die Protokolle bereits eine gewisse Resistenz gegen Angriffe zeigen. Da es im Gegensatz zu vielen Routingprotokollen keine oder sehr wenig direkte Signalisierung zwischen den Fahrzeugen gibt, fallen viele Angriffsmöglichkeiten schlicht weg. Der Angreifer ist im Wesentlichen auf Denial-of-Service Angriffe oder das Verfälschen der Information beschränkt.

Damit versagen aber auch herkömmliche, auf Kryptographie-basierende Sicherheitsmechanismen[2]. Solche Mechanismen setzen vor allem auf einen Sender-basierten Schutz, bei dem der Sender einer Nachricht diese durch Signaturen vor Veränderungen oder durch Verschlüsselung vor Ausspähung schützt. Weiterhin gehen diese oft von einem statischen Paketinhalt aus, der unverändert oder mit wenigen Veränderungen im Header durch das Netzwerk verschickt wird. Während letzteres zumindest bei Gossiping noch zutrifft, kann die Information bei Context-adaptive Message Dissemination bereits beim Versenden neu in Pakete gepackt werden und beim Einsatz von Aggregationsverfahren geht die Einzelinformation vollkommen verloren.

Der Sender- und Paketzentrierte Ansatz muss deshalb durch einen Daten-orientierten Ansatz erweitert bzw. ersetzt werden. Hier kommen Mechanismen wie Konsistenzchecks zum Einsatz, welche die Plausibilität der Informationen und die Konsistenz der Informationen bei redundanter Verteilung oder mehrerer Informationsquellen prüfen. Vorhandene Sensoren wie RADAR oder LIDAR können für zusätzliche Konsistenzchecks genutzt werden.

Werden Inkonsistenzen erkannt, die auf einen Angriff hindeuten, so kommen reaktive Sicherheitsmechanismen zum Einsatz, die gefälschte Daten erkennen und verwerfen, die Verteilung durch Erhöhung der Redundanz robuster gegen Angriffe machen oder in anderer Weise auf den erkannten Angriff reagieren. Beispielsweise können Ratenkontrollmechanismen verhindern, dass einzelne Knoten das Netz mit Informationen fluten, um eine Überlastsituation zu erreichen.

Abbildung 1 zeigt die Auswirkungen eines Angriffs auf die kontext-adaptive Nachrichtenverteilung, wenn der Angreifer gefälschte Nachrichten mit hoher Rate absetzt. Anhand der Färbung kann man sehen, dass sich dadurch die Queues von Knoten in der Umgebung des Angreifers nach und nach mit gefälschten Nachrichten füllen. Der Angreifer ist also in der Lage, die reguläre Kommunikation in einer gewissen Umgebung sehr stark zu stören.

IV. Zusammenfassung und Ausblick

Zusammenfassend lässt sich sagen, dass die genannten Kommunikationsformen erfolgreich die Effizienz der Fahrzeug-Fahrzeug Kommunikation verbessern und dabei die Anpassung an stark wechselnde Fahrzeugdichten ermöglichen.

Gleichzeitig zeigen unsere Untersuchungen, dass die Mechanismen per se bereits eine gewisse Sicherheit gegenüber Angriffen bieten. Zum Schutz gegen Angriffen können insbesondere Konsistenzprüfungen und Ratenkontrollmechanismen beitragen. Wir sind zur Zeit dabei, derartige Mechanismen zu entwerfen und zu evaluieren.

Literatur

[1] Christian Maihöfer, "A Survey Of Geocast Routing Protocols," *IEEE Communications Surveys*, vol. 6, no. 2, pp. 32–42, 2004.

[2] Holger Füssler, Martin Mauve, Hannes Hartenstein, Michael Käsemann, and Dieter Vollmer, "A Comparison of Routing Strategies for Vehicular Ad Hoc Networks," Department of Computer Science, University of Mannheim, Technical Report TR-3-2002, Jul. 2002.

[3] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *VANET '07*. New York, NY, USA: ACM, September 2007, pp. 19–28.

[2]wobei zur Verhinderung von Sybil-Angriffen nach wie vor eine Authentisierung gültiger Fahrzeuge notwendig ist.

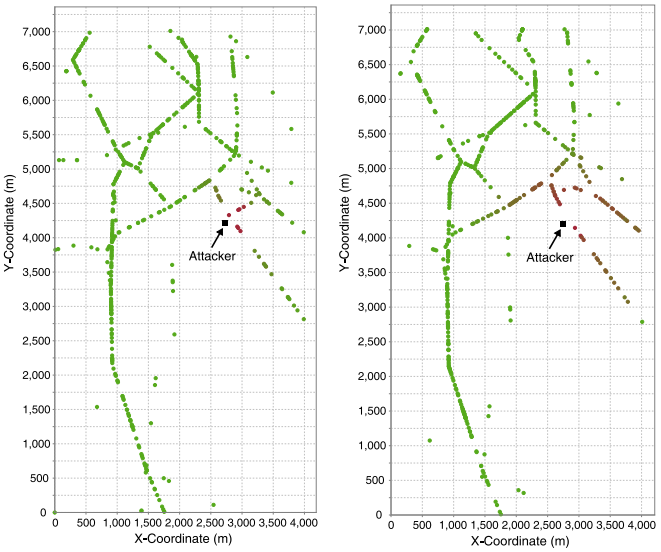

Abbildung 1. Verlauf eines Angriffs auf Context-adaptive message dissemination, bei dem der Angreifer gefälschte Nachrichten mit hoher Frequenz absetzt - Status der Queues nach 20s (links) und 50s (rechts)

[4] E. Schoch, F. Kargl, T. Leinmüller, and M. Weber, "Vulnerabilities of geocast message distribution," in *2nd IEEE Workshop on Automotive Networking and Applications (AutoNet 2007, in conj. with GlobeCom 2007)*, Washington, DC, USA, Nov. 2007.

[5] J. Luo, P. Eugster, and J. Hubaux, "Route driven gossip: Probabilistic reliable multicast in ad hoc networking," in *Infocom*, 2003.

[6] Markus Strassberger, Christian Adler, and Robert Eigner, "Situationsadaptive Verbreitung von Kontextinformationen in automobilen Ad-hoc-Netzen," *Praxis der Informationsverarbeitung und Kommunikation*, vol. 1, no. 29, pp. 43–49, Mar. 2006.

Charakteristika von Katastrophenszenarien

Nils Aschenbruck, Elmar Gerhards-Padilla, Peter Martini
Universität Bonn - Institut für Informatik IV
Römerstr. 164, 53117 Bonn, Deutschland
{aschenbruck, padilla, martini}@cs.uni-bonn.de

I. Einleitung und Motivation

Vor nicht allzu langer Zeit gab es eine Vielzahl Szenarien, die als potentielle Einsatzgebiete für Mobile multihop Ad-hoc NETze (MANETs) gesehen wurden (vgl. u.a. [1]). Bei einigen dieser Szenarien kann davon ausgegangen werden, dass es sich nicht mehr nur um *potentielle* Szenarien handelt, da erste Produkte, die MANET-Technologien beinhalten, kommerziell eingesetzt werden. Eines dieser Szenarien ist das so genannte Katastrophenszenario. Das von den Katastrophenschutz-Einheiten benutzte Kommunikationssystem basiert somit im Katastrophenszenario auf einem MANET.

Da MANETs in Katastrophenszenarien zum Einsatz kommen, ist es für die weitere Forschung und Entwicklung in diesem Bereich wichtig, Besonderheiten und Charakteristika von Katastrophenszenarien zu kennen. Das Ziel dieses Beitrags ist es daher ebendiese Besonderheiten und Charakteristika von Katastrophenszenarien zu analysieren.

Die Leistungsbewertung von Algorithmen und Protokollen für MANETs erfolgt überwiegend simulativ. Daher werden die Ergebnisse einer simulativen Leistungsbewertung stark von der modellierten Bewegung und Last beeinflusst. Im folgenden werden Besonderheiten und Charakteristika von Bewegung (Abschnitt II), Datenverkehr (Abschnitt III) sowie der Verteilung des Datenverkehrs auf die sich bewegenden Knoten (Abschnitt IV) für Katastrophenszenarien erläutert werden.

II. Bewegung in Katastrophenszenarien

Katastrophen können nicht nur sehr komplex sondern auch sehr unterschiedlich sein. Allerdings arbeitet der Katastrophenschutz auch in verschiedenen Lagen nach einem grundlegenden Konzept, der so genannten *taktischen Gliederung des Raumes* (vgl. [2]). Dieses Konzept beinhaltet die Einteilung des Schadensgebietes in taktische Räume. Um größere Schadenslagen führen zu können, wird quasi ein “Divide-and-Conquer”-Ansatz verfolgt. Dieses abstrakte Konzept erlaubt durch seine Skalierbarkeit die Beherrschung beliebig komplexer Schadenslagen.

Jede Einheit wird entsprechend ihrer Qualifikation in einem taktischen Raum eingesetzt. Bei einer sanitätsdienstlichen Lage könnte ein Feuerwehrmann beispielsweise an einer Schadensstelle zum Befreien von eingeklemmten Personen eingesetzt werden, während ein Sanitäter in einer der Stellen des Behandlungsbereiches eingesetzt werden könnte. Dies bedeutet, dass sich die Einheiten nicht beliebig über die gesamte Fläche bewegen, sondern die Bewegung der Einheiten durch den taktischen Raum bestimmt wird, dem sie zugeteilt sind.

Bei der spezifischen Bewegung einer Einheit, ist es entscheidend, ob es sich um eine stationäre Einheit oder eine Transporteinheit handelt. Für stationäre Einheiten begrenzt der taktische Raum, dem die Einheit zugeordnet ist, die Bewegung. Für Transporteinheiten z.B. Trage-Trupps oder Rettungsmittel ist die Bewegung durch verschiedene taktische Räume bestimmt. Patienten werden zum Beispiel von der Verletztenablage zum Behandlungsplatz transportiert. Dazu bewegt sich ein Trage-Trupp den Patienten auf einer Trage transportierend von der Verletztenablage zum Behandlungsplatz.

Innerhalb der einzelnen Räume gibt es keine relevanten Hindernisse. Bis auf die Schadensstellen wird die Position der taktischen Räume von der Einsatzleitung festgelegt, so dass Hindernisse vermieden werden. Im Schadensgebiet werden Hindernisse, die die Bewegung beeinflussen, zerstört. Hindernisse beeinflussen also lediglich die Bewegung der Transporteinheiten zwischen den Räumen. Diese Einheiten bewegen sich auf einem optimalen Weg. Eine Transporteinheit wird folglich einen möglichst kurzen und Hindernisse vermeidenden Weg wählen.

Für längere Patienten-Transporte, zum Beispiel vom Behandlungsplatz zum Krankenhaus, werden Rettungsmittel eingesetzt. Somit kommen in diesem Szenario Knoten unterschiedlicher Geschwindigkeit vor. Darüber hinaus verlassen die Rettungsmittel das Katastrophenszenario, da Krankenhäuser im Allgemeinen weiter entfernt liegen und nicht Teil des Kommunikationssystems im Katastrophengebiet sind. Aus dem Verlassen dieser Transporteinheiten (Rettungsmittel) folgt, dass entsprechend weitere Einheiten (Rettungsmittel) nachgefordert werden, die dann später zum Szenario hinzukommen.

Wenn man also die Bewegung in Katastrophengebieten basierend auf dem Konzept der Gliederung des Raumes genauer analysiert, ergeben sich insgesamt die folgenden Eigenschaften:

- Heterogene Bewegung, die die taktischen Räume berücksichtigt
- Bewegung auf optimalen Pfaden, die Hindernisse vermeiden
- Einige Einheiten verlassen das Netz, andere kommen hinzu

Diese grundlegenden Eigenschaften wurden im so genannten Disaster-Area-Bewegungsmodell [3] berücksichtigt. Bei

diesem werden taktische Räume definiert und die einzelnen Knoten diesen zugeordnet, wodurch zugleich eine geographische Restriktion der Bewegung erfolgt. Basierend auf einem Ansatz aus der Bewegungsplanung für Roboter (Sichtbarkeitsgraphen) werden optimale Pfade zwischen den Hindernissen berücksichtigt, die den Bewegungs-Zyklus der einzelnen Knoten beeinflussen. Das Ein- und Ausschalten der Knoten wird durch eine Erweiterung des Bewegungsformates realisiert.

III. Datenverkehr in Katastrophenszenarien

Die klassische Anwendung in Kommunikationssystemen für Katastrophenszenarien ist der Sprachdatenverkehr. Dabei handelt es sich im Wesentlichen um Push-to-Talk-Gruppenkommunikation. Das neue BOS-Funksystem basierend auf dem TETRA-Standard ermöglicht neben Sprachdatenverkehr auch Paketdatenverkehr. Für die Paketdatendienste werden verschiedene Anwendungen erwartet. Diese stimmen im Wesentlichen mit den im Rahmen des Projekt MESA (Mobility for Emergency and Safety Applications) spezifizierten Anforderungen bezüglich der gewünschten Applikationen überein [4]. Insgesamt werden für zukünftige Netze folgenden Anwendungen erwartet: Sprache, Informationssysteme, E-Mail, Bilder, Videos sowie Sensor-Informationen.

Der Anteil und die Relevanz der verschiedenen Anwendungen für zukünftige Netze sind schwer abzuschätzen, da in Katastrophen heute fast ausschließlich Sprachdaten verwendet werden. Sprachdaten haben besondere Anforderungen an die Qualität der Datenübertragung (z.B. geringe Verzögerung und Jitter), sodass gerade Sprachdaten für eine aussagekräftige Leistungsbewertung realistisch modelliert werden sollten. Die übertragenen Informationen mögen in der Zukunft die "Verpackung" (Codec, etc.) ändern, zentrale Kommunikationscharakteristika werden aber erhalten bleiben.

Bei der Modellierung des Datenverkehrs (vgl. [5]) sind insbesondere konversationelle Abhängigkeiten zu berücksichtigen. Die Kommunikation erfolgt zwar über Multicast-Funkrufe, dennoch sind Konversationen zu beobachten. Dies impliziert, dass Funkrufe gehäuft auftreten. Innerhalb der Konversationen kommt es zu kleineren IDLE-Zeiten, wohingegen zwischen den Konversationen größere IDLE-Zeiten zu beobachten sind.

IV. Verteilung des Datenverkehrs in Katastrophenszenarien

In Katastrophenszenarien wird, wie im vorangegangenen Abschnitt beschrieben, im wesentlichen Multicast-Sprachdatenverkehr verwendet. Dabei gibt es sowohl lokale wie auch globale Kommunikationsgruppen. Lokale Kommunikationsgruppen kommunizieren innerhalb eines taktischen Raumes, wie zum Beispiel eines Behandlungsplatzes. Dahingegen dienen globale Kommunikationsgruppen der Kommunikation zwischen verschiedenen Bereichen. Ein Beispiel hierfür ist ein allgemeiner Führungskanal.

Da es sich um Broadcast-Sprachdatenverkehr innerhalb einer Gruppe handelt, stellen alle Knoten einer Kommunikationsgruppe Lastsenken der Funksprüche dieser Gruppe dar. In Katastrophenszenarien liegt also die Herausforderung in der realistischen Verteilung der Lastquellen.

Die Kommunikation verschiedener Gruppenteilnehmer wird durch festgelegte Verkehrsformen bestimmt (vgl. [6]). Verkehrsformen sind Kommunikationsmuster, die bestimmen welche Stationen direkt miteinander kommunizieren dürfen. Für Katastrophengebiete sind die folgenden Verkehrsformen relevant:

- *Mesh-Kommunikation*: Jeder Teilnehmer darf mit jedem anderen kommunizieren. Die Teilnehmer sind gleichberechtigt.
- *Stern-Kommunikation*: Es gibt einen Teilnehmer mit Leitfunktion (Sternkopf). Jeder Teilnehmer darf ausschließlich mit diesem Teilnehmer kommunizieren. Die Kommunikation zu anderen Teilnehmern ist nicht erlaubt.

Im Katastrophenfall ist zur Bewältigung der Informationsflut ausschließlich Stern-Kommunikation vorgesehen. Da aber technisch auch Mesh-Kommunikation möglich ist, neigen die Teilnehmer teilweise dazu, auch wenn dies explizit nicht erlaubt ist, dem Stern-Kommunikationsmuster nicht immer zu folgen. Dies bedeutet, dass sich in der Realität bei Beobachtung des Funkverkehrs keine reinen Kommunikationsmuster wiederfinden.

In [7] wurde basierend auf Messungen in Katastrophenschutzübungen gezeigt, dass mehr als 80% der Funkrufe dem Stern-Kommunikationsmuster folgen. Für die Verteilung der Funksprüche auf die Lastquellen (Teilnehmer einer Gruppe) folgt daraus, dass ein wesentlich größerer Anteil der Funksprüche von einer Station, dem Sternkopf, initiiert wird.

V. Zusammenfassung

Insgesamt zeigt sich, dass in Katastrophenszenarien Bewegung, Datenverkehr und Verteilung der Lastquellen spezifische Charakteristika aufzeigen. Diese sollten bei der Leistungsbewertung in MANETs - sofern die Algorithmen und Protokolle auch in Katastrophenszenarien zum Einsatz kommen sollen - berücksichtigt werden.

References

[1] C. E. Perkins, *Ad Hoc Networking*. Addison-Wesley, 2001.

[2] *KatS-DV 100 - Führung und Leitung im Einsatz*, Ständige Konferenz für Katastrophenvorsorge und Katastrophenschutz (SKK), 1999, http://www.katastrophenvorsorge.de/pub/publications/DV100-SKK.pdf.

[3] N. Aschenbruck, E. Gerhards-Padilla, M. Gerharz, M. Frank, and P. Martini, "Modelling Mobility in Disaster Area Scenarios," *Proc. 10th ACM-IEEE Int. Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM)*, pp. 4–12, 2007.

[4] *TS 70.001 V3.2.1 Technical Specification - Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)*, MESA, 2006.

[5] N. Aschenbruck, M. Gerharz, M. Frank, and P. Martini, "Modelling Voice Communication in Disaster Area Scenarios," *Proc. IEEE Conf. on Local Computer Networks (LCN2006)*, pp. 211–220, 2006.

[6] *KatS-DV 810 - Sprechfunkdienst*, Bundesamt für Zivilschutz (BZS), 1977, http://gsb.download.bva.bund.de/BBK/KatS_Dv_810.pdf.

[7] N. Aschenbruck, M. Gerharz, and P. Martini, "How to Assign Traffic Sources to Nodes in Disaster Area Scenarios," *Proc. of the 26th IEEE Intern. Performance Computing and Communications Conf. (IPCCC)*, 2007.

Sicherheit in taktischen MANETs

Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini
Universität Bonn - Institut für Informatik IV
Römerstr. 164, 53117 Bonn, Deutschland
{padilla, aschenbruck, martini}@cs.uni-bonn.de

I. Einleitung und Motivation

Vor einigen Jahren waren mobile multihop Ad-hoc Netze (MANETs) noch ein reines Forschungsthema. Dies hat sich mit der Einführung erster MANET-Technologie enthaltender kommerzieller Produkte inzwischen geändert. Insbesondere für militärische und Katastrophenszenarien sind solche Produkte inzwischen verfügbar.
Gerade in solchen Szenarien ist Sicherheit von besonderer Relevanz, da mit hoher Wahrscheinlichkeit von der Anwesenheit feindlicher oder terroristischer Einheiten ausgegangen werden kann. Das Ziel dieses Beitrags ist es Sicherheitsrisiken in MANETs aufzuzeigen und zwei Verfahren zur Erkennung von Angriffen gegen MANETs vorzustellen.
Im Folgenden werden zunächst taktische MANETs und ihre Besonderheiten eingeführt (Abschnitt II). Anschließend werden die Sicherheitsrisiken in MANETs kategorisiert, (Abschnitt III) sowie die Verfahren Topology Graph based Anomaly Detection (TOGBAD) (Abschnitt IV) und Cluster based Anomaly Detection (CBAD) (Abschnitt V) vorgestellt.

II. Taktische MANETs

Unter taktischen MANETs versteht man im Kontext von militärischen oder Katastrophenzenarien eingesetzte MANETs. Solche taktischen MANETs unterscheiden sich anhand von zwei Punkten von allgemeinen MANETs:
Zum einen ist in solchen Szenarien mit hoher Wahrscheinlichkeit von feindlichen Einheiten oder Terroristen auszugehen. Dies führt sowohl zu einem erhöhten Risiko einer Übernahme legitimierter Knoten durch Angreifer, als auch zu besonders schwerwiegenden Folgen erfolgreicher Angriffe, da im schlimmsten Fall sogar menschliche Verluste auftreten können.
Zum anderen existiert in taktischen Szenarien eine Kommandostruktur unter den Knoten. Es existieren voll ausgerüstete und leichtgewichtige Knoten. Die voll ausgerüsteten Knoten sind im Allgemeinen geographisch zurückgelagert und verfügen über Zugang zu Stromversorgung und leistungsfähige Hardware (z.B. Laptops oder ähnliches). Die leichtgewichtigen Knoten verwenden hingegen im Allgemeinen batteriebetriebene, weniger leistungsstarke Hardware (z.B. PDAs oder ähnliches).

III. Sicherheitsrisiken in MANETs

In MANETs existiert eine Vielzahl von Sicherheitsrisiken. Diese Sicherheitsrisiken lassen sich in die drei folgenden Gruppen einteilen:

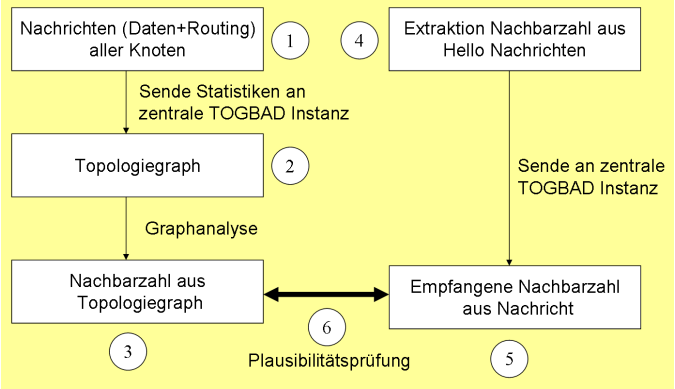

Abbildung 1. Funktionsweise TOGBAD

- Spezielle Relevanz in MANETs
  Hierbei handelt es sich um Sicherheitsrisiken, die aufgrund der Eigenschaften von MANETs besondere Relevanz aufweisen. Sie führen dazu, dass bestimmte Angriffe in solchen Netzen deutlich leichter durchführbar sind als in Festnetzen. Ein Beispiel hierfür sind Angriffe gegen das Routing, so genannte Routingangriffe. Da jeder Knoten in das Routing im MANET eingebunden ist, fällt es einem Knoten im Vergleich zu Festnetzen leicht, bösartig Einfluss auf das Routing zu nehmen.
- Bekannt auf Festnetzen
  In dieser Gruppe werden die aus Festnetzen bekannten Sicherheitsrisiken, wie Denial of Service (DoS) Angriffe oder Würmer zusammengefasst. Schwachstellen in eingesetzten Protokollen oder Betriebssystemen können in MANETs wie in Festnetzen ausgenutzt werden. Deshalb sind aus Festnetzen bekannte Angriffe auch in MANETs relevant.
- Drahtlose Netze
  Unter diese Kategorie fallen die aufgrund des drahtlosen Mediums auftretenden Sicherheitsrisiken. Das in MANETs verwendete Medium erlaubt sowohl das Mithören des im Netz versendeten Verkehrs, als auch die gezielte Störung des Mediums, z.B. über Jamming der verwendeten Funkfrequenzen.

IV. TOGBAD

TOGBAD (vgl. [1]) dient zur Erkennung von Sicherheitsrisiken mit spezieller Relevanz in MANETs, speziell zur Detektion von Angriffen gegen das MANET-Routing-Protokoll.

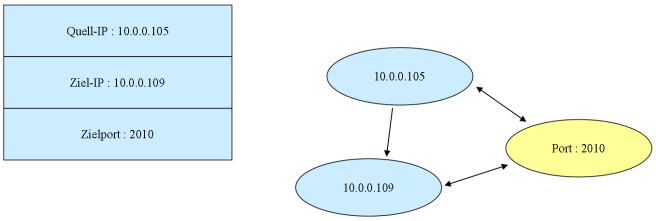

Abbildung 2. Grapherzeugung CBAD

Die Idee von TOGBAD besteht darin, an einer zentralen Stelle Topologieinformationen über das vorliegende Netz zu sammeln. Auf Basis dieser Topologieinformationen wird dann eine globale Plausibilitätsprüfung der im Netz versendeten Routing-Nachrichten durchgeführt.
Zur Erlangung der Topologieinformationen senden die leichtgewichtigen Knoten periodisch Informationen über die im Netz übertragenen Pakete an einen voll ausgestatteten Knoten. Auf diesem voll ausgestatteten Knoten läuft eine TOGBAD-Instanz, die aus den empfangenen Informationen einen Topologiegraphen generiert (vgl. Abbildung 1 Schritte 1-3).
Zusätzlich werden von den leichtgewichtigen Knoten Meldungen über die von ihren Nachbarn versendeten Routingnachrichten an eine TOGBAD-Instanz gesendet (vgl. Abbildung 1 Schritte 4,5). Die TOGBAD-Instanz ist somit in der Lage die Routingnachrichten anhand des Topologiegraphen auf Plausibilität zu prüfen (vgl. Abbildung 1 Schritt 6). Dies geschieht mit Hilfe von Anomalieerkennung. Weicht die in einer Routingnachricht propagierte Topologie zu stark vom Abbild der tatsächlichen Topologie im Topologiegraphen ab, so wird ein Alarm generiert. Zu stark heißt in diesem Fall, dass die Differenz zwischen propagierter und tatsächlicher Topologie außerhalb des mittels statistischer Methoden berechneten Akzeptanzintervalls liegt.
Erste Evaluationen zur Erkennungsleistung von TOGBAD in taktischen MANETs finden sich in [1] und [2].

V. CBAD

CBAD (vgl. [4], [3]) ist ein Verfahren, das ursprünglich für die Erkennung von Angriffen in Festnetzen entwickelt worden ist. Erste Untersuchngen seiner grundsätzlichen Eignung auch für MANETs und Evaluationen in MANETs finden sich in [5] und [6]. Auch in MANETs ist CBAD in der Lage DoS-Angriffe und Würmer zu erkennen und stellt somit ein Erkennungsverfahren für die zweite Gruppe von Sicherheitsrisiken aus Abschnitt III dar.
Bei CBAD handelt es sich um ein graphbasiertes Anomalieerkennungsverfahren. Alle am Netzwerk beteiligten Stationen werden als Knoten in einem Graphen dargestellt. Für jedes im Netzwerk verschickte Datenpaket wird – sofern noch nicht vorhanden – eine Kante zwischen Quell- und Zielknoten erstellt bzw. die bereits existierende Kante stärker gewichtet. Dabei werden die IP-Adressen der Verbindungen betrachtet. Nach einer festgelegten Zeit (Runde) wird dieser Vorgang beendet, der Graph aufgearbeitet („geclustert“) und die Struktur des Graphen analysiert. Deutliche Änderungen dieser Struktur im Vergleich mit vorher erstellten Graphen deuten nun auf eine Anomalie hin. Die Abweichung der Struktur wird als so genannter Diff-Wert gemessen. Es existieren zwei Erweiterungen dieser Grundfunktion von CBAD. Mit Hilfe der ersten Erweiterung können zusätzlich die Zielports der Datenpakete von CBAD verarbeitet und als zusätzliche Knoten in den Graphen eingefügt werden. Ein Beispiel der Grapherzeugung von CBAD bei Verwendung der Porterweiterung befindet sich in Abbildung 2. Mit dieser Erweiterung ist es möglich, ungewöhnlich hohes Verkehrsaufkommen an einem Port zu erkennen. Die zweite Erweiterung ist eine Hyperaktivitäts-Erkennung von CBAD. Weicht das Kommunikationsaufkommen eines Knoten stark vom Normalzustand ab, so wird dieser Knoten als hyperaktiv gewertet.

VI. Zusammenfassung

In dieser Arbeit wurden zunächst die Besonderheiten von taktischen MANETs eingeführt. Diese erlauben eine zentralisierte Vorgehensweise bei der Erkennung von Angriffen. Die bei Verwendung von MANETs vorhandenen Sicherheitsrisiken wurden kategorisiert und für zwei der eingeführten Gruppen mit TOGBAD und CBAD Verfahren zur Detektion vorgestellt. Beides sind graphbasierte Anomalieerkennungsverfahren. TOGBAD dient zur Erkennung von Routingangriffen, CBAD detektiert DoS-Angriffe und Würmer. Beide Verfahren können wertvolle Bausteine für ein Intrusion-Detection-System für taktische MANETs darstellen.

Literatur

[1] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke und J. Tölle, “Detecting Blackhole Attacks in Tactical MANETs using Topology Graphs”, Proc. of LCN Workshop on Network Security (WNS), 2007.
[2] B. Gerner, “Graph-basierte IDS-Detektoren für taktische MANETs – Implementierung, Integration und Evaluation”, Diplomarbeit, Abt. IV, Inst. f. Informatik, Universität Bonn, 2007.
[3] Jens Toelle, Marko Jahnke, Nils gentschen Felde, Peter Martini, “Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System”, Proc. of IEEE Military Communications Conference (MILCOM), 2006.
[4] J. Tölle, “Intrusion Detection durch strukturbasierte Erkennung von Anomalien im Netzverkehr”, Dissertation, Universität Bonn. GCA-Verlag, 2002.
[5] M. Jahnke und J. Tölle, A. Finkenbrink, and A. Wenzel, 2. Zwischenbericht, Projektdokumentation zum Forschungsvorhaben "MANET Intrusion Detection for Tactical Environments"(MITE), Phase II, Im Auftrage des Bundesamtes fuer Informationsmanagement und Informationstechnik der Bundeswehr, Koblenz, 2007.
[6] M. Jahnke und J. Tölle, A. Finkenbrink, and A. Wenzel, 3. Zwischenbericht, Projektdokumentation zum Forschungsvorhaben "MANET Intrusion Detection for Tactical Environments"(MITE), Phase II, Im Auftrage des Bundesamtes fuer Informationsmanagement und Informationstechnik der Bundeswehr, Koblenz, 2007.

Dynamic Buffer Management Scheme Based on Hop Count for Ad Hoc Networks

Mohamed Abd rabou Kalil and Andreas Mitshele-Thiel
Integrated HW/SW Systems Group
Ilmenau University of Technology
98693 Ilmenau, Germany
Email: mohamed.abdrabou, mitsch@tu-ilmenau.de

***Abstract*— In this paper, we propose an efficient buffer management scheme for ad hoc networks. This scheme is based on virtual partitioning of the buffer at each node according to the number of hops that the packet traversed from source node to the relaying node. The partitions are correlated and dynamically changed according to the traffic load. Moreover, the proposed scheme guarantees a certain level of quality of service (QoS) for real time packets and energy status of the relaying node. An analytical model based on a *4-dimensional* Markov chain and simulation are carried out. The results show that the proposed scheme outperforms the other schemes in terms of end-to-end delay and loss probability.**

I. Introduction

Most existing buffer management schemes like drop-tail and random-early detection (RED) [1] do not take the number of hops into account when dropping the packet, which leads to routing message overhead and end-to-end delay for long hops (LH) flows . In [2], we proved that, using network simulator 2 (NS2) [3], the aforementioned queue management schemes and some other schemes fail to present fairness to LH flows because of the previous reason. Presenting fairness for all traffic types is a challenge in multihop networks. The fairness from our point of view means, how can a fair buffer access for LH flows and short hops (SH) flows can be developed. For ease of illustration, suppose a big disaster like tsunami or tornado happened in a place crowded by people. Also, it is supposed that there is no infrastructure to find out what the current situation is, in this place?. The rescue workers battling a disaster may use multihop ad hoc network to reach the nearest access point. Therefore, packets that are coming from a far place must be given a high priority to access the buffer of the relaying nodes. To achieve this goal, an efficient buffer management must be developed to present fairness for all traffic types. Several buffer management schemes [4] have been proposed to satisfy fairness for all traffic types under different load conditions. None of those schemes presents a suitable algorithm for multihop ad hoc network.

This paper proposes a buffer management scheme for tackling the fairness among diverse of traffic named Hop-Aware Buffering (HAB). HAB is based on virtual partitioning of the buffer according to the number of hops the packets will traversed from source to the relaying node. Those partitions can grow and shrink, therefore they are dynamically changed according to traffic load. When the buffer is full, packets are dropped or pushed out based on the state of the buffer's partitions. This is done to obtain a better utilization of the buffer. The service priorities (scheduling) are to be done according the following criteria: the number of hops that the packet will traversed from the relaying node to its destination, the importance of the packet (real time or non-real time) and the energy status of the relaying node.

II. Hop-Aware Buffering (HAB)

In this section, the description of HAB will be presented as follows. Let N be the total number of nodes equipped with ad hoc network. Let M denoting the maximum number of hops that can be occurred by a packet within a network. The number of hops can be determined from the routing table at each node. Let $l = 0, 1, 2, \ldots, M$ be the number of hops that a packets traversed from source to the current node. As illustrated in Figure 1, HAB scheme consists of four components. Namely, classifier, queue manager, partitioned buffer and scheduler. Each node has a finite-capacity buffer with size B to host the arriving packets.

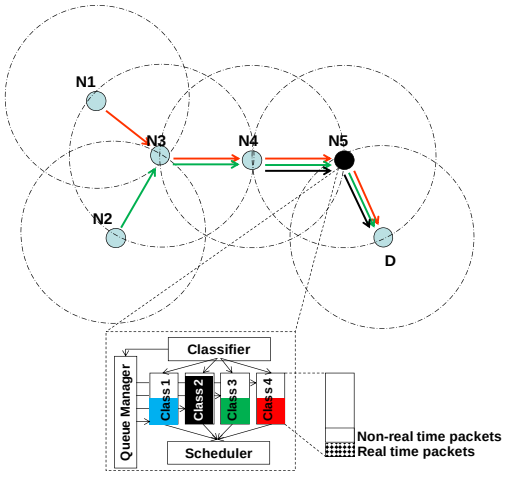

Fig. 1. Multihop ad hoc network using HAB scheme.

The classifier is responsible for classifying the incoming packet into either one of four classes according to the number of traversed hops l from source to the current node. If $1 \leq l < h$ then a packet is classified as class-1, if $h \leq l < 2h - 1$ then a packet is classified as class-2, if

$2h-1 \leq l < 2\,(h+1)$ then a packet is classifies as class-3 and if $2\,(h+1) \leq l \leq M$ then a packet is classified as class-4, where $h = \lceil \frac{N}{3} \rceil$

The total buffer size is divided initially into four virtual partitions, each partition serve one class. The size of each partition n, $T(n), n = 1,\ 2,\ 3,\ 4$ is computed as the total buffer size divide by 4, that is $T(n) = \frac{B}{4}$. From the first look at Figure 1, it appears that the size of each partition is fixed, but that is not true. The partitions are correlated and dynamically changed according to the traffic load of each class, to have a better utilization of the buffer.

After a packet is classified, the queue manager will be responsible for accepting, dropping and pushing out the packet. With accepting, that means there is available space for this packet. With dropping, that means there is no available space for it. With pushing out, that means the queue manager will push out another packet to accept the newly arriving packet.

In our proposed scheme, the scheduler decides which packet will be served first based on some metrics. Namely, the number of hops, QoS guarantee and energy status of the hosting node. In this paper, the scheduler's decision will be done according to the number of hops only. Other metrics will be done in the future work.

A. HAB Description

Upon a packet (from any class) arrives at the buffer, one of the following four possible cases may be happened:

- Case 1: a packet arrives at the node and find an available space in its appropriate partition, henceforth called destination partition. In such case, the packet will be accepted.
- Case 2: a packet arrives at the node and finds no available buffer space in its destination partition and all other partitions (buffer is full). In such case, the packet will be rejected if all partitions have the same size.
- Case 3: a packet arrives at the node and there is no space available in its destination partition but there is space available in the other partitions. In such case, the queue manager will determine the partition with a maximum free space, henceforth called source partition, where *free space = partition size - the number of packets in it*. Once the source partition is determined, one buffer space from it is moved to the destination partition and then the packet is accepted.
- Case 4: a packet arrives at the node and there is no available space in its destination partition and all other partitions like case 2, but the partitions had different sizes. Then, the queue manager will determine for the longest one, push out one packet from it and move the free space into the destination partition and then the incoming packet is accepted.

III. Results and Conclusion

A mathematical model based on *4-dimensional* Markov chain process has been developed. The results have been validated using a JAVA discrete-event simulator. The scenario that we tested is organized as shown in Figure 1, where all nodes send packets to same destination D. In Figure 2, the end-to-end delay for LH flow is very low in HAB scheme, compared to the default scheme. However, the performance of SH flow is greater than the default scheme. From our point of view, this enhancement reduced the network cost because the LH flow had a good chance to access the node buffer, therefore the LH packets retransmission will be reduced. Figure 3 illustrates the theoretical and simulated loss probability for LH flow for both HAB and drop tail schemes. As seen from the figure, HAB scheme decreases the loss probability for LH flow in low and high traffic, which resulted in reducing the communication overhead.

In future, we planned to consider the effect of energy consumed in each node. The study of combined effect of all involved factors (number of hops, packets importance and energy in each relaying node) to reduce the cost is expected to provide much better results.

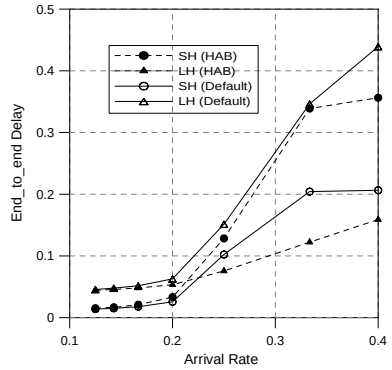

Fig. 2. End-to-end delay vs. arrival rate for HAB and default scheme

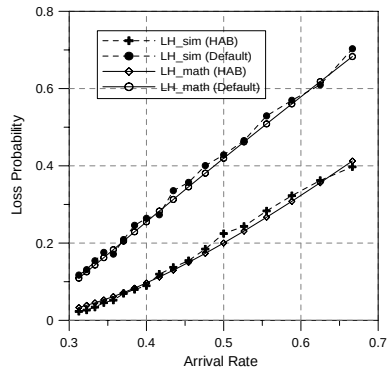

Fig. 3. Loss probability vs. arrival rate for HAB and default scheme

References

[1] S. Floyd and V. Jacobson, "Random Early Detection gateways for Congestion Avoidance," IEEE/ACM Transactions on Networking, vol. 1, 1993, pp. 397-413.

[2] M. A. Kalil, N. Zamin-Khan, H. Al Mahdi and A. Mitschele-Thiel, "Evaluation and Improvement of Queueing Management Schemes in Multihop Ad hoc Networks," 52 Internationales Wissenschaftliches Kolloquium (52-IWK), Ilmenau, Germany, vol. 2, 2007, pp. 397-402.

[3] "The Network Simulator ns2," http://www.isi.edu/nsnam/ns/.

[4] S. Dijkstra, "Modeling Active Queue Management algorithms using Stochastic Petri Nets," Master Thesis, University of Twente, 2004.

Liste der bisher erschienenen Ulmer Informatik-Berichte

Einige davon sind per FTP von `ftp.informatik.uni-ulm.de` erhältlich
Die mit * markierten Berichte sind vergriffen

List of technical reports published by the University of Ulm

Some of them are available by FTP from `ftp.informatik.uni-ulm.de`
Reports marked with * are out of print

91-01 *Ker-I Ko, P. Orponen, U. Schöning, O. Watanabe*
Instance Complexity

91-02* *K. Gladitz, H. Fassbender, H. Vogler*
Compiler-Based Implementation of Syntax-Directed Functional Programming

91-03* *Alfons Geser*
Relative Termination

91-04* *J. Köbler, U. Schöning, J. Toran*
Graph Isomorphism is low for PP

91-05 *Johannes Köbler, Thomas Thierauf*
Complexity Restricted Advice Functions

91-06* *Uwe Schöning*
Recent Highlights in Structural Complexity Theory

91-07* *F. Green, J. Köbler, J. Toran*
The Power of Middle Bit

91-08* *V.Arvind, Y. Han, L. Hamachandra, J. Köbler, A. Lozano, M. Mundhenk, A. Ogiwara, U. Schöning, R. Silvestri, T. Thierauf*
Reductions for Sets of Low Information Content

92-01* *Vikraman Arvind, Johannes Köbler, Martin Mundhenk*
On Bounded Truth-Table and Conjunctive Reductions to Sparse and Tally Sets

92-02* *Thomas Noll, Heiko Vogler*
Top-down Parsing with Simulataneous Evaluation of Noncircular Attribute Grammars

92-03 *Fakultät für Informatik*
17. Workshop über Komplexitätstheorie, effiziente Algorithmen und Datenstrukturen

92-04* *V. Arvind, J. Köbler, M. Mundhenk*
Lowness and the Complexity of Sparse and Tally Descriptions

92-05* *Johannes Köbler*
Locating P/poly Optimally in the Extended Low Hierarchy

92-06* *Armin Kühnemann, Heiko Vogler*
Synthesized and inherited functions -a new computational model for syntax-directed semantics

92-07* *Heinz Fassbender, Heiko Vogler*
A Universal Unification Algorithm Based on Unification-Driven Leftmost Outermost Narrowing

92-08* *Uwe Schöning*
On Random Reductions from Sparse Sets to Tally Sets

92-09* *Hermann von Hasseln, Laura Martignon*
Consistency in Stochastic Network

92-10 *Michael Schmitt*
A Slightly Improved Upper Bound on the Size of Weights Sufficient to Represent Any Linearly Separable Boolean Function

92-11 *Johannes Köbler, Seinosuke Toda*
On the Power of Generalized MOD-Classes

92-12 *V. Arvind, J. Köbler, M. Mundhenk*
Reliable Reductions, High Sets and Low Sets

92-13 *Alfons Geser*
On a monotonic semantic path ordering

92-14* *Joost Engelfriet, Heiko Vogler*
The Translation Power of Top-Down Tree-To-Graph Transducers

93-01 *Alfred Lupper, Konrad Froitzheim*
AppleTalk Link Access Protocol basierend auf dem Abstract Personal Communications Manager

93-02 *M.H. Scholl, C. Laasch, C. Rich, H.-J. Schek, M. Tresch*
The COCOON Object Model

93-03 *Thomas Thierauf, Seinosuke Toda, Osamu Watanabe*
On Sets Bounded Truth-Table Reducible to P-selective Sets

93-04 *Jin-Yi Cai, Frederic Green, Thomas Thierauf*
On the Correlation of Symmetric Functions

93-05 *K.Kuhn, M.Reichert, M. Nathe, T. Beuter, C. Heinlein, P. Dadam*
A Conceptual Approach to an Open Hospital Information System

93-06 *Klaus Gaßner*
Rechnerunterstützung für die konzeptuelle Modellierung

93-07 *Ullrich Keßler, Peter Dadam*
Towards Customizable, Flexible Storage Structures for Complex Objects

94-01 *Michael Schmitt*
On the Complexity of Consistency Problems for Neurons with Binary Weights

94-02 *Armin Kühnemann, Heiko Vogler*
A Pumping Lemma for Output Languages of Attributed Tree Transducers

94-03 *Harry Buhrman, Jim Kadin, Thomas Thierauf*
On Functions Computable with Nonadaptive Queries to NP

94-04 *Heinz Faßbender, Heiko Vogler, Andrea Wedel*
Implementation of a Deterministic Partial E-Unification Algorithm for Macro Tree Transducers

94-05 *V. Arvind, J. Köbler, R. Schuler*
On Helping and Interactive Proof Systems

94-06 *Christian Kalus, Peter Dadam*
Incorporating record subtyping into a relational data model

94-07 *Markus Tresch, Marc H. Scholl*
A Classification of Multi-Database Languages

94-08 *Friedrich von Henke, Harald Rueß*
Arbeitstreffen Typtheorie: Zusammenfassung der Beiträge

94-09 *F.W. von Henke, A. Dold, H. Rueß, D. Schwier, M. Strecker*
Construction and Deduction Methods for the Formal Development of Software

94-10 *Axel Dold*
Formalisierung schematischer Algorithmen

94-11 *Johannes Köbler, Osamu Watanabe*
New Collapse Consequences of NP Having Small Circuits

94-12 *Rainer Schuler*
On Average Polynomial Time

94-13 *Rainer Schuler, Osamu Watanabe*
Towards Average-Case Complexity Analysis of NP Optimization Problems

94-14 *Wolfram Schulte, Ton Vullinghs*
Linking Reactive Software to the X-Window System

94-15 *Alfred Lupper*
Namensverwaltung und Adressierung in Distributed Shared Memory-Systemen

94-16 *Robert Regn*
Verteilte Unix-Betriebssysteme

94-17 *Helmuth Partsch*
Again on Recognition and Parsing of Context-Free Grammars:
Two Exercises in Transformational Programming

94-18 *Helmuth Partsch*
Transformational Development of Data-Parallel Algorithms: an Example

95-01 *Oleg Verbitsky*
On the Largest Common Subgraph Problem

95-02 *Uwe Schöning*
Complexity of Presburger Arithmetic with Fixed Quantifier Dimension

95-03 *Harry Buhrman,Thomas Thierauf*
The Complexity of Generating and Checking Proofs of Membership

95-04 *Rainer Schuler, Tomoyuki Yamakami*
Structural Average Case Complexity

95-05 *Klaus Achatz, Wolfram Schulte*
Architecture Indepentent Massive Parallelization of Divide-And-Conquer Algorithms

95-06 *Christoph Karg, Rainer Schuler*
Structure in Average Case Complexity

95-07 *P. Dadam, K. Kuhn, M. Reichert, T. Beuter, M. Nathe*
ADEPT: Ein integrierender Ansatz zur Entwicklung flexibler, zuverlässiger kooperierender Assistenzsysteme in klinischen Anwendungsumgebungen

95-08 *Jürgen Kehrer, Peter Schulthess*
Aufbereitung von gescannten Röntgenbildern zur filmlosen Diagnostik

95-09 *Hans-Jörg Burtschick, Wolfgang Lindner*
On Sets Turing Reducible to P-Selective Sets

95-10 *Boris Hartmann*
Berücksichtigung lokaler Randbedingung bei globaler Zieloptimierung mit neuronalen Netzen am Beispiel Truck Backer-Upper

95-12 *Klaus Achatz, Wolfram Schulte*
Massive Parallelization of Divide-and-Conquer Algorithms over Powerlists

95-13 *Andrea Mößle, Heiko Vogler*
Efficient Call-by-value Evaluation Strategy of Primitive Recursive Program Schemes

95-14 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
A Generic Specification for Verifying Peephole Optimizations

96-01 *Ercüment Canver, Jan-Tecker Gayen, Adam Moik*
Formale Entwicklung der Steuerungssoftware für eine elektrisch ortsbediente Weiche mit VSE

96-02 *Bernhard Nebel*
Solving Hard Qualitative Temporal Reasoning Problems: Evaluating the Efficiency of Using the ORD-Horn Class

96-03 *Ton Vullinghs, Wolfram Schulte, Thilo Schwinn*
An Introduction to TkGofer

96-04 *Thomas Beuter, Peter Dadam*
Anwendungsspezifische Anforderungen an Workflow-Mangement-Systeme am Beispiel der Domäne Concurrent-Engineering

96-05 *Gerhard Schellhorn, Wolfgang Ahrendt*
Verification of a Prolog Compiler - First Steps with KIV

96-06 *Manindra Agrawal, Thomas Thierauf*
Satisfiability Problems

96-07 *Vikraman Arvind, Jacobo Torán*
A nonadaptive NC Checker for Permutation Group Intersection

96-08 *David Cyrluk, Oliver Möller, Harald Rueß*
An Efficient Decision Procedure for a Theory of Fix-Sized Bitvectors with Composition and Extraction

96-09 *Bernd Biechele, Dietmar Ernst, Frank Houdek, Joachim Schmid, Wolfram Schulte*
Erfahrungen bei der Modellierung eingebetteter Systeme mit verschiedenen SA/RT–Ansätzen

96-10 *Falk Bartels, Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Formalizing Fixed-Point Theory in PVS

96-11 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Mechanized Semantics of Simple Imperative Programming Constructs

96-12 *Axel Dold, Friedrich W. von Henke, Holger Pfeifer, Harald Rueß*
Generic Compilation Schemes for Simple Programming Constructs

96-13 *Klaus Achatz, Helmuth Partsch*
From Descriptive Specifications to Operational ones: A Powerful Transformation Rule, its Applications and Variants

97-01 *Jochen Messner*
Pattern Matching in Trace Monoids

97-02 *Wolfgang Lindner, Rainer Schuler*
A Small Span Theorem within P

97-03 *Thomas Bauer, Peter Dadam*
A Distributed Execution Environment for Large-Scale Workflow Management Systems with Subnets and Server Migration

97-04 *Christian Heinlein, Peter Dadam*
Interaction Expressions - A Powerful Formalism for Describing Inter-Workflow Dependencies

97-05 *Vikraman Arvind, Johannes Köbler*
On Pseudorandomness and Resource-Bounded Measure

97-06 *Gerhard Partsch*
Punkt-zu-Punkt- und Mehrpunkt-basierende LAN-Integrationsstrategien für den digitalen Mobilfunkstandard DECT

97-07 *Manfred Reichert, Peter Dadam*
$ADEPT_{flex}$ - Supporting Dynamic Changes of Workflows Without Loosing Control

97-08 *Hans Braxmeier, Dietmar Ernst, Andrea Mößle, Heiko Vogler*
The Project NoName - A functional programming language with its development environment

97-09 *Christian Heinlein*
Grundlagen von Interaktionsausdrücken

97-10 *Christian Heinlein*
Graphische Repräsentation von Interaktionsausdrücken

97-11 *Christian Heinlein*
Sprachtheoretische Semantik von Interaktionsausdrücken

97-12 *Gerhard Schellhorn, Wolfgang Reif*
Proving Properties of Finite Enumerations: A Problem Set for Automated Theorem Provers

97-13 *Dietmar Ernst, Frank Houdek, Wolfram Schulte, Thilo Schwinn*
Experimenteller Vergleich statischer und dynamischer Softwareprüfung für eingebettete Systeme

97-14 *Wolfgang Reif, Gerhard Schellhorn*
Theorem Proving in Large Theories

97-15 *Thomas Wennekers*
Asymptotik rekurrenter neuronaler Netze mit zufälligen Kopplungen

97-16 *Peter Dadam, Klaus Kuhn, Manfred Reichert*
Clinical Workflows - The Killer Application for Process-oriented Information Systems?

97-17 *Mohammad Ali Livani, Jörg Kaiser*
EDF Consensus on CAN Bus Access in Dynamic Real-Time Applications

97-18 *Johannes Köbler,Rainer Schuler*
Using Efficient Average-Case Algorithms to Collapse Worst-Case Complexity Classes

98-01 *Daniela Damm, Lutz Claes, Friedrich W. von Henke, Alexander Seitz, Adelinde Uhrmacher, Steffen Wolf*
Ein fallbasiertes System für die Interpretation von Literatur zur Knochenheilung

98-02 *Thomas Bauer, Peter Dadam*
Architekturen für skalierbare Workflow-Management-Systeme - Klassifikation und Analyse

98-03 *Marko Luther, Martin Strecker*
A guided tour through *Typelab*

98-04 *Heiko Neumann, Luiz Pessoa*
Visual Filling-in and Surface Property Reconstruction

98-05 *Ercüment Canver*
Formal Verification of a Coordinated Atomic Action Based Design

98-06 *Andreas Küchler*
On the Correspondence between Neural Folding Architectures and Tree Automata

98-07 *Heiko Neumann, Thorsten Hansen, Luiz Pessoa*
Interaction of ON and OFF Pathways for Visual Contrast Measurement

98-08 *Thomas Wennekers*
Synfire Graphs: From Spike Patterns to Automata of Spiking Neurons

98-09 *Thomas Bauer, Peter Dadam*
Variable Migration von Workflows in *ADEPT*

98-10 *Heiko Neumann, Wolfgang Sepp*
Recurrent V1 – V2 Interaction in Early Visual Boundary Processing

98-11 *Frank Houdek, Dietmar Ernst, Thilo Schwinn*
Prüfen von C–Code und Statmate/Matlab–Spezifikationen: Ein Experiment

98-12 *Gerhard Schellhorn*
Proving Properties of Directed Graphs: A Problem Set for Automated Theorem Provers

98-13 *Gerhard Schellhorn, Wolfgang Reif*
Theorems from Compiler Verification: A Problem Set for Automated Theorem Provers

98-14 *Mohammad Ali Livani*
SHARE: A Transparent Mechanism for Reliable Broadcast Delivery in CAN

98-15 *Mohammad Ali Livani, Jörg Kaiser*
Predictable Atomic Multicast in the Controller Area Network (CAN)

99-01 *Susanne Boll, Wolfgang Klas, Utz Westermann*
A Comparison of Multimedia Document Models Concerning Advanced Requirements

99-02 *Thomas Bauer, Peter Dadam*
Verteilungsmodelle für Workflow-Management-Systeme - Klassifikation und Simulation

99-03 *Uwe Schöning*
On the Complexity of Constraint Satisfaction

99-04 *Ercument Canver*
Model-Checking zur Analyse von Message Sequence Charts über Statecharts

99-05 *Johannes Köbler, Wolfgang Lindner, Rainer Schuler*
Derandomizing RP if Boolean Circuits are not Learnable

99-06 *Utz Westermann, Wolfgang Klas*
Architecture of a DataBlade Module for the Integrated Management of Multimedia Assets

99-07 *Peter Dadam, Manfred Reichert*
Enterprise-wide and Cross-enterprise Workflow Management: Concepts, Systems, Applications. Paderborn, Germany, October 6, 1999, GI–Workshop Proceedings, Informatik ’99

99-08 *Vikraman Arvind, Johannes Köbler*
Graph Isomorphism is Low for ZPP^{NP} and other Lowness results

99-09 *Thomas Bauer, Peter Dadam*
Efficient Distributed Workflow Management Based on Variable Server Assignments

2000-02 *Thomas Bauer, Peter Dadam*
Variable Serverzuordnungen und komplexe Bearbeiterzuordnungen im Workflow-Management-System ADEPT

2000-03 *Gregory Baratoff, Christian Toepfer, Heiko Neumann*
Combined space-variant maps for optical flow based navigation

2000-04 *Wolfgang Gehring*
Ein Rahmenwerk zur Einführung von Leistungspunktsystemen

2000-05 *Susanne Boll, Christian Heinlein, Wolfgang Klas, Jochen Wandel*
Intelligent Prefetching and Buffering for Interactive Streaming of MPEG Videos

2000-06 *Wolfgang Reif, Gerhard Schellhorn, Andreas Thums*
Fehlersuche in Formalen Spezifikationen

2000-07 *Gerhard Schellhorn, Wolfgang Reif (eds.)*
FM-Tools 2000: The 4th Workshop on Tools for System Design and Verification

2000-08 *Thomas Bauer, Manfred Reichert, Peter Dadam*
Effiziente Durchführung von Prozessmigrationen in verteilten Workflow-Management-Systemen

2000-09 *Thomas Bauer, Peter Dadam*
Vermeidung von Überlastsituationen durch Replikation von Workflow-Servern in ADEPT

2000-10 *Thomas Bauer, Manfred Reichert, Peter Dadam*
Adaptives und verteiltes Workflow-Management

2000-11 *Christian Heinlein*
Workflow and Process Synchronization with Interaction Expressions and Graphs

2001-01 *Hubert Hug, Rainer Schuler*
DNA-based parallel computation of simple arithmetic

2001-02 *Friedhelm Schwenker, Hans A. Kestler, Günther Palm*
3-D Visual Object Classification with Hierarchical Radial Basis Function Networks

2001-03 *Hans A. Kestler, Friedhelm Schwenker, Günther Palm*
RBF network classification of ECGs as a potential marker for sudden cardiac death

2001-04 *Christian Dietrich, Friedhelm Schwenker, Klaus Riede, Günther Palm*
Classification of Bioacoustic Time Series Utilizing Pulse Detection, Time and Frequency Features and Data Fusion

2002-01 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
Effiziente Verträglichkeitsprüfung und automatische Migration von Workflow-Instanzen bei der Evolution von Workflow-Schemata

2002-02 *Walter Guttmann*
Deriving an Applicative Heapsort Algorithm

2002-03 *Axel Dold, Friedrich W. von Henke, Vincent Vialard, Wolfgang Goerigk*
A Mechanically Verified Compiling Specification for a Realistic Compiler

2003-01 *Manfred Reichert, Stefanie Rinderle, Peter Dadam*
A Formal Framework for Workflow Type and Instance Changes Under Correctness Checks

2003-02 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
Supporting Workflow Schema Evolution By Efficient Compliance Checks

2003-03 *Christian Heinlein*
Safely Extending Procedure Types to Allow Nested Procedures as Values

2003-04 *Stefanie Rinderle, Manfred Reichert, Peter Dadam*
On Dealing With Semantically Conflicting Business Process Changes.

2003-05 *Christian Heinlein*
Dynamic Class Methods in Java

2003-06 *Christian Heinlein*
Vertical, Horizontal, and Behavioural Extensibility of Software Systems

2003-07 *Christian Heinlein*
Safely Extending Procedure Types to Allow Nested Procedures as Values
(Corrected Version)

2003-08 *Changling Liu, Jörg Kaiser*
Survey of Mobile Ad Hoc Network Routing Protocols)

2004-01 *Thom Frühwirth, Marc Meister (eds.)*
First Workshop on Constraint Handling Rules

2004-02 *Christian Heinlein*
Concept and Implementation of C+++, an Extension of C++ to Support User-Defined Operator Symbols and Control Structures

2004-03 *Susanne Biundo, Thom Frühwirth, Günther Palm(eds.)*
Poster Proceedings of the 27th Annual German Conference on Artificial Intelligence

2005-01 *Armin Wolf, Thom Frühwirth, Marc Meister (eds.)*
19th Workshop on (Constraint) Logic Programming

2005-02 *Wolfgang Lindner (Hg.), Universität Ulm , Christopher Wolf (Hg.) KU Leuven*
2. Krypto-Tag – Workshop über Kryptographie, Universität Ulm

2005-03 *Walter Guttmann, Markus Maucher*
Constrained Ordering

2006-01 *Stefan Sarstedt*
Model-Driven Development with ACTIVECHARTS, Tutorial

2006-02 *Alexander Raschke, Ramin Tavakoli Kolagari*
Ein experimenteller Vergleich zwischen einer plan-getriebenen und einer leichtgewichtigen Entwicklungsmethode zur Spezifikation von eingebetteten Systemen

2006-03 *Jens Kohlmeyer, Alexander Raschke, Ramin Tavakoli Kolagari*
Eine qualitative Untersuchung zur Produktlinien-Integration über Organisationsgrenzen hinweg

2006-04 *Thorsten Liebig*
Reasoning with OWL - System Support and Insights –

2008-01 *H.A. Kestler, J. Messner, A. Müller, R. Schuler*
On the complexity of intersecting multiple circles for graphical display

2008-02 *Manfred Reichert, Peter Dadam, Martin Jurisch,l Ulrich Kreher, Kevin Göser, Markus Lauer*
Architectural Design of Flexible Process Management Technology

2008-03 *Frank Raiser*
Semi-Automatic Generation of CHR Solvers from Global Constraint Automata

2008-04 *Ramin Tavakoli Kolagari, Alexander Raschke, Matthias Schneiderhan, Ian Alexander*
Entscheidungsdokumentation bei der Entwicklung innovativer Systeme für produktlinien-basierte Entwicklungsprozesse

2008-05 *Markus Kalb, Claudia Dittrich, Peter Dadam*
Support of Relationships Among Moving Objects on Networks

2008-06 *Matthias Frank, Frank Kargl, Burkhard Stiller (Hg.)*
WMAN 2008 – KuVS Fachgespräch über Mobile Ad-hoc Netzwerke

Ulmer Informatik-Berichte
ISSN 0939-5091

Herausgeber:
Universität Ulm
Fakultät für Ingenieurwissenschaften und Informatik
89069 Ulm