Abstract Proceedings of the 7th Workshop on Wireless and Mobile Ad-Hoc Networks (WMAN 2013)

Matthias Frank, Frank Kargl, Burkhard Stiller

Ulmer Informatik-Berichte

Nr. 2013-01
März 2013

Ulmer Informatik Berichte | Universität Ulm | Fakultät für Ingenieurwissenschaften und Informatik

WMAN 2013

7th Workshop on

Wireless and Mobile Ad-Hoc Networks

http://wman2013.cs.uni-bonn.de/

in conjunction with Networked Systems (NetSys) 2013

Welcome to the seventh edition of our Workshop on Wireless and Mobile Ad-Hoc Networks. Based on the success of the preceding WMAN workshops of 2011 back to 2002, the workshop was again held on March 11, 2013 in conjunction with the bi-annual conference Networked Systems 2013 (formerly the ITG/GI conference on communication in distributed systems, German: ITG/GI - Fachtagung "Kommunikation in Verteilten Systemen").

Wireless and Mobile Ad-Hoc Networking covers a broad variety of applications, including areas like mesh networking, wireless sensor networks, vehicular networks, personal area networks, some forms of body area net-works, and many more. Over the years, the field diversified and many newly emerging application areas now constitute research fields of their own. WMAN 2013 seeks to provide a platform for a broad discussion among researchers from all these diverse fields. Thereby, we want to enhance awareness of new trends and approaches in other areas of ad-hoc networking.

With the change from KiVS to NetSys, we also changed the format of the WMAN workshop. While in previous years we solicited full papers that underwent detailed peer-review, we now switched to a less formal and more interactive approach. Submissions were solicited only in abstract form and underwent a relevancy check. We explicitly asked also for submissions that provide a broader picture on the work of a working group or a specific community or raise new issues or challenges that the research community should discuss during the workshop.

This years program features a provoking keynote by Nils Aschenbruck on "Ad-hoc Networking – Blue Sky Research forever?" followed by 5 presentations on aspects like routing overhead, security, ad-hoc integration with cellular networks, and context-adaptive networking.

The presentations in detail:

We hope that workshop participants will enjoy these interesting topics and engage in intensive discussions.

Stuttgart, March 11, 2013

Matthias Frank, Frank Kargl, Burkhard Stiller

Ad-hoc Networking – Blue Sky Research forever?

Nils Aschenbruck
University of Osnabrück
Institute of Computer Science
Albrechtstr. 28
49076 Osnabrück, Germany
aschenbruck@uos.de

Blue sky research is scientific research in domains where real applications and markets seem not to be existing. Some people see ad-hoc networking as one of the domains that have this "problem" On the one hand, they may be right. Mobile Ad-hoc Networks are standardized for more than 15 years now (cf. RFC-2501). But we have not seen products that really dominate the markets. On the other hand, there are products, solutions, and still open challenges. - From the research side, blue skies are needed for real innovation. Thus, a domain with plenty blue sky seems to be great.

The keynote will review the ad-hoc networking blue sky phenomena by surveying selected application domains as well as products that have made it to market. Then, the possible reasons, challenges, and solutions concerning blue skies are presented. Finally, some research challenges and future directions for ad-hoc networking are highlighted.

Predicting Optimized Link State Routing Protocol Control Message Overhead in MANETs

Sascha Jopen, Raphael Ernst
University of Bonn
Institute of Computer Science 4
Bonn, Germany
{jopen, ernst}@cs.uni-bonn.de

***Abstract*—Since several years MANETs are a hot topic in research. There are several routing protocols available for MANETs and for nearly every protocol further extensions and improvements exist, which often require particular configurations for optimal operation. The problem of finding an ideal parameter set for a given network scenario is often solved with time-consuming network simulations. However, real world deployments of Mobile Adhoc Networks (MANETs) require a timely determination of suitable parameters. Therefore, we propose an analytical approach to help finding appropriate parameters for a given scenario and to reduce the complexitiy of simulations. Our work is focused on the widely used OLSR routing protocol. The overall performance of an OLSR network is highly influenced by the transmission interval of topology control messages. Depending on the mobility of the nodes and the available bandwidth, shorter or longer intervals are more appropriate. Our analytical results presented in this paper allow for a precise estimation of the load imposed by OLSR control messages for each node. This eliminates the need of time-consuming simulations to choose appropriate intervals for control messages. Furthermore, these predictions could be a basis for automatic protocol configuration during runtime.**

***Index Terms*—MANET, OLSR, routing, overhead, prediction**

I. Introduction

The Optimized Link State Routing Protocol (OLSR) [1] is a popular routing protocol for MANETs. As a proactive routing protocol it maintains routes to all possible destinations all the time. Like classical Link State Routing Protocols (LSRs), OLSR performs neighbor detection and advertises links in the network with two different message types. HELLO messages are used to discover links to neighboring nodes, while Topology Control (TC) messages are used to disseminate this topology information throughout the network. By combining each node's neighbor information obtained through TC messages and the local neighborhood discovered with HELLO messages, a node can calculate routes to all other nodes in the network.

The intervals at which HELLO and TC messages are generated and transmitted are configurable parameters of OLSR. They can greatly influence the performance of the routing protocol. As shown in [2], decreasing the HELLO and TC intervals improves the reaction times of OLSR with respect to route availability. However, shorter message intervals imply higher routing overhead. Especially when using High Frequency (HF) radios or similar with data rates of only a few kbit/s the additional overhead can easily overload the channels.

Finding optimal parameter sets for arbitrary scenarios regarding message intervals is a challenging task. Often network simulations are leveraged to determine these parameters. However, running several simulations for different parameter sets with the required amount of replications can be quite time-consuming. The predictions presented in this paper allow for a precise estimation of the incoming load caused by TC messages, individually for each node. The only input required are the communications ranges of all nodes, as well as node positions and movements. Calculating the predicted load is a lot faster than running exhaustive simulations. Furthermore, this could be used to adapt TC intervals dynamically to the available channel capacity.

The rest of this paper is structured as follows: In section II other work related to the subject of this paper is presented. In section III MPR selector paths are defined, a fundamental concept for estimating the incoming control message load for nodes. In section IV our analytical model is explained in detail. In section V the performance of our predictions compared to simulation results is presented and discussed. Finally, in section VI we draw a conclusion.

II. Related Work

Most of the publications presenting optimizations for routing protocols make use of network simulations to show and verify the changes proposed. However, there are also a few publications, which introduce analytical approches to estimate the protocol behaviours. Nguyen and Minet estimate in [3] the overhead introduced by OLSR HELLO and TC messages. Based on the average number of neighbors for each node and the average number of Multipoint-Relays (MPRs) in a network with evenly distributed nodes in a square area, the routing protocol overhead within the entire network is calculated. Extracting more detailed information, which node contributes how much load to the overhead is not possible.

In [4], Jiang et al. briefly approximate the impact of OLSR message interval optimizations on the routing protocol overhead in terms of transmitted packets. Both HELLO and TC messages are considered. Based on [5], the average number of MPRs in a network and the configured message emission intervals are used to estimate the number of control messages transmitted in the whole network. Though this gives a rough overview of the overhead, deriving per node statistics is impossible as well.

Medina and Bohacek present in [6] detailed models for the fractions of nodes generating, forwarding, and receiving TC messages. A comparison of the execution times for calculating the estimated overhead shows a significant speedup compared to the simulations used for validation. Though the models allow for a detailed analysis of the overall performance of the MPR flooding mechanism, they are not suitable for calculating the expected incoming message load of particular nodes.

III. MPR Selector Paths

In contrast to HELLO messages, which are not forwarded, TC messages have to be broadcasted and forwarded to all nodes in the OLSR network. To reduce network traffic and the risk of broadcast storms [7], an optimized forwarding technique called MPR flooding [8] is employed. Here, forwarding of control messages is done only by some of the nodes, the MPRs, thus reducing the amount of retransmitted packets. MPRs are selected by their surrounding neighbor nodes. A node a selecting another node b as an MPR is called an MPR selector of b.

$$\begin{aligned} G &= (V, E) \\ V &= \{\text{all nodes in the network}\} \\ E &= \{(u,v) \in V^2 \mid v \text{ is MPR selector of } u\} \end{aligned} \tag{1}$$

The directed graph G defined in (1) containing all nodes as vertices and edges from all MPRs to their respective MPR selectors is further referred to as the MPR selector graph. Each directed path from a given node to another node is called an MPR selector path. Control messages transmitted by an end node of such an MPR selector path will eventually reach the start node, as each node's predecessor on the path is an MPR for it and thus forwards the messages. Therefore, a node will receive control messages from all other nodes to which an MPR selector path exists.

Symbol	Definition
$\text{Size}_{\text{Tc}}(m)$	Size of a TC message, generated by node m in bytes.
$\text{Size}_{\text{MsgHdr}}$	OLSR message header size: 12 bytes.
$\text{Size}_{\text{TcHdr}}$	TC message header size: 4 bytes.
$\text{Size}_{\text{TcAddr}}$	Size of a single address in TC messages: 4 bytes.
$N_{\text{Advertised}}(m)$	Set of all neighbors of node m, which are in its *Advertised Neighbor Set*.
$N_{\text{MPR}}(m)$	Set of all MPR neighbors of node m.
$\text{Tc}_{\text{Interval}}$	TC message interval in seconds.
$M_{\max}(y)$, $M_{\min}(y)$	Maximum/minimum number of TC message bytes sent by node y.
$\text{MPR}_{\text{SP}}(y)$	Set of MPR nodes, reachable by MPR selector paths starting from node y, including y.
$\text{MPR}_{\text{SP*}}(y)$	Set of nodes from $\text{MPR}_{\text{SP}}(y)$, excluding $\text{MPR}_{\text{SP}}(z)$ with $z \in N_{\text{Sym}}(y)$ and z not MPR selector of y, including y.
$\text{Links}_{\text{Asym}}(y, x)$	Set of links with node x is in communication range of node y.

TABLE I
Symbols used for the predictions.

IV. Predictions

The following formulas describe the expected load imposed by TC messages on a given node. All symbols used in the formulas are summarized in Table I. Though OLSR allows for partial TC messages, it is assumed that all topology information of a node is transmitted within a single OLSR message. Only the size of the actual TC messages including the general OLSR message header is considered. Additional OLSR packet headers, UDP, IP and lower layer headers are irrelevant for this analysis but can easily be added if desired.

$$\begin{aligned} \text{Size}_{\text{Tc}}(m) = {} & \text{Size}_{\text{MsgHdr}} + \text{Size}_{\text{TcHdr}} \\ & + \text{Size}_{\text{TcAddr}} \cdot |N_{\text{Advertised}}(m)| \end{aligned} \tag{2}$$

The size of a TC message originated at a node m, given in equation (2), is the sum of the general OLSR message header, the TC header and the sum of the size of an IPv4 address times the number of neighbors advertised in the TC message of node m. Every node advertises at least all of its neighbors, which are MPR selectors of the node. Optionally, the nodes can additionally advertise their own MPRs, or all of their neighbors. The set of the advertised nodes is called the Advertised Neighbor Set.

$$M_{\max}(y) = \sum_{m \in \text{MPR}_{\text{SP}}(y)} \frac{\text{Size}_{\text{Tc}}(m)}{\text{Tc}_{\text{Interval}}} \tag{3}$$

$$M_{\min}(y) = \sum_{m \in \text{MPR}_{\text{SP*}}(y)} \frac{\text{Size}_{\text{Tc}}(m)}{\text{Tc}_{\text{Interval}}} \tag{4}$$

The formulas (3) and (4) calculate the maximum and minimum outgoing load in bytes per second transmitted by a given MPR node y. For each MPR m reachable using an MPR selector path starting at node y, the average number of bytes per second of TC messages originated at node m is calculated, which is the size of a TC message divided by the interval in which they are sent. The corresponding TC messages are eventually received by y and potentially forwarded. Node y itself generates TC messages. Even though they are not forwarded by y, they are sent by y nevertheless and thus included in the sum. As TC messages are only generated by MPRs, nodes which are not selected as an MPR by some other node, are not considered.

Due to the fact that, according to RFC 3626, section 3.4.1 (2), an MPR node retransmits a message only if it receives the message for the first time from one of its MPR selectors over a given interface, there are two similar formulas. The first one assumes that all control messages are always received from one of the MPR selectors and thus are always forwarded. The second formula on the other hand assumes that all messages are first received from a node, which is not an MPR selector. These messages are not forwarded. Often, many MPR nodes have only neighbors, which are both MPRs themselves and MPR selectors of the node, or not MPRs at all. That is, the control messages can only reach these nodes from one of its MPR selectors. All control messages are always forwarded by these nodes. The equations (3) and (4) are equivalent for this type of nodes. MPRs for which it is not clear whether they will forward an incoming message beforehand are further referred to as critical MPRs.

$$\text{L}_{\max}(x) = \sum_{y \in N_{\text{MPR}}(x)} (|\text{Links}_{\text{Asym}}(y,x)| \cdot M_{\max}(y)) \tag{5}$$

Parameter	Configuration
Number of nodes	16
Node distances	50 m
PHY & MAC layer model	IEEE 802.11g
Communication Range	fixed, 60 m
Data rate	fixed, 54 Mbit/s
HELLO Interval	2 s
Neighbor Hold Time	6 s
TC Interval	5 s
Topology Hold Time	15 s
Advertised Neighbor Set of each node	All neighbors which are MPR selectors of this node.
Simulation time	900 s (Discarding the first 30 s)

TABLE II
SIMULATION PARAMETERS.

$$\text{L}_{\min}(x) = \sum_{y \in N_{\text{MPR}}(x)} (|\text{Links}_{\text{Asym}}(y,x)| \cdot M_{\min}(y)) \tag{6}$$

The formulas (5) and (6) finally calculate the maximum and minimum load of TC messages in bytes per second received by an arbitrary node x. As TC messages are only generated and forwarded by MPRs, only the neighboring nodes of x which are MPRs account for the load received by x. All messages are received over every asymmetric link from the MPR neighbors to node x, which is important in multi-device OLSR configurations. An asymmetric link denotes a link between two nodes, where communication is only possible in one direction. This basically means that it is sufficient for node x to be in communication range of other MPRs to receive the messages forwarded and generated by them. As a consequence of the formulas (3) and (4) there exists a predicted maximum and minimum load caused by TC messages.

$$\text{L}_{\min}(x) \leq \text{L}(x) \leq \text{L}_{\max}(x) \tag{7}$$

In summary the above formulas lead to equation (7) with an expected incoming TC message load for a node x somewhere in between the minimum and maximum predicted TC message load for this node. Because the difference between minimum and maximum predicted load solely depends on messages arriving for the first time at an MPR either from an MPR selector or from another node, the actually measured load heavily depends on the propagation delay of the messages within the network.

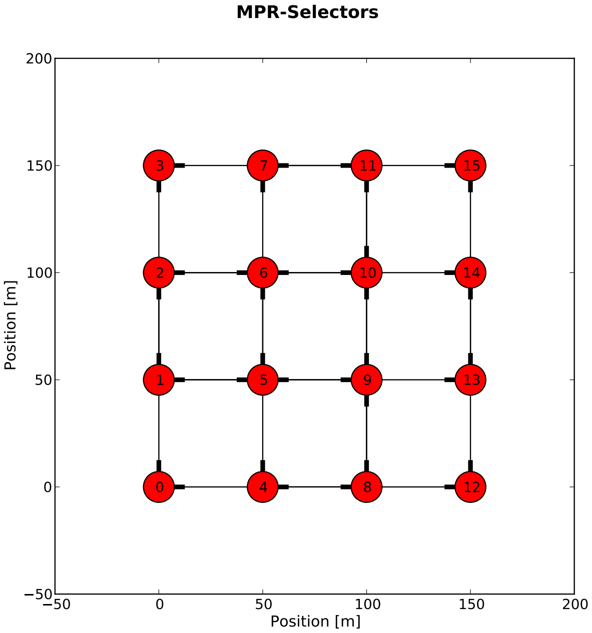


Fig. 1. Visualization of the static grid scenario with MPR selector paths. An edge from a node x to node y implies y is MPR selector of x, that is x forwards control messages received from y.

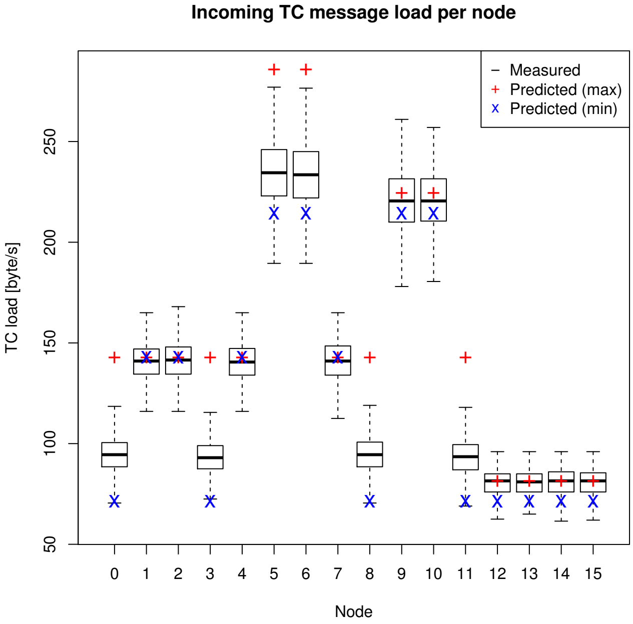


Fig. 2. Predicted TC message load versus measured load in the static grid scenario (cf. Fig. 1).

V. Evaluation

The predictions as presented in section IV were evaluated and verified in several static scenarios of different sizes simulated with ns-3 [9] and a Click Modular Router [10] based OLSR implementation, developed at our department.

The results for simulations of a grid scenario with 16 nodes are presented in this section. The nodes are positioned 50 m apart with no node mobility. All nodes are equipped with a single wireless interface with a fixed communication range of 60 m. Each node advertises only their MPR selectors in TC messages. This setup leads to a network topology as depicted in Fig. 1. Each node in the simulation runs a full featured OLSR instance with default parameters as described in RFC 3626. The actually received number of TC messages and their sizes are measured, summed up in discrete time intervals and filtered using a moving average to reduce peaks caused by message bursts. The first 30 s of simulation time were skipped to allow for stabilization of OLSR. All relevant simulation parameters are outlined in Table II. We conducted ten replications of this simulation. Running a single simulation takes approximatly 15 s, while the computation of the predicted loads takes less than 200 ms. Even if the predictions are calculated for time steps with one second resolution, which would be necessary for scenarios with mobile nodes or otherwise changing topology, less than 5 s are spent for computation.

The input parameters for our predictions were derived from the node positions and the communication ranges only. Because of the fixed transmission ranges no explicit link detection has to be modeled. Symmetric links between all nodes within communication range are assumed instead. A standalone MPR selection algorithm, implementing the RFC 3626 MPR selection, calculates the MPR set for each node. Using this information a graph containing all MPR selector paths is constructed, which is used to compute the formulas.

The results of the simulations described above and the corresponding predicted load is depicted in Fig. 2. The actual load was measured for time steps of one second resolution. The filtered data points for all replications are drawn as a boxplot for each node.

Variations in the incoming loads are caused by jitter, propagation delay and packet loss due to collisions. Every control message is sent in fixed intervals minus some random jitter. This can lead to incoming load bursts when packets are generated nearly at the same time by several different nodes, which is the main reason for the incoming load deviation. The more MPR neighbors a node has the higher is the deviation, which can be observed for all nodes. Due to the propagation delay of messages, critical MPRs will sometimes receive messages, originated at another node, for the first time from an MPR selector and sometimes not. This yields higher load for intervals when the message is received from an MPR selector and lesser load otherwise. This can be observed for the nodes 0, 3, 8, and 11, as well as nodes 5 and 6. Depending on the probability of messages arriving either from an MPR selector or not, and thus on the structure of the network, the actual load lies more toward the minimum or maximum predicted load. Furthermore, every node in the simulated scenario can suffer from packet loss caused by the hidden terminal problem [11] because no node is in transmission range of any other adjacent node of one of its neighbors. As these effects are not modeled by our predictions, the expected maximum load is always greater or equal than the average actual load. This is best observed at nodes 1, 2, 4, and 7, however, every node is affected.

Obviously, the predicted and the measured loads match very well, especially at nodes with identical or nearly identical minimum and maximum expected loads. The actual load in case of differing minimum and maximum predicted loads for a node is mainly influenced by the order in which packets arrive at a neighboring MPR, and thus the propagation delay of packets. As this is currently not modelled by the predictions the difference between the minimum and maximum predicted loads can be quite large. How large this difference is, depends on the number of nodes reachable by MPR selector paths starting from neighboring critical MPRs. For example, the nodes 5 and 6, as well as the nodes 9 and 10 all have four neighboring MPRs, each of them having exactly one critical MPR. Thus, the minimum predicted load is the same for all. The maximum load, however, is different, because the critical MPRs 4 and 7 always receive TC messages from all other nodes in the networks over their links to node 8 or 11, respectively. The critical MPRs 13 and 14 on the other hand only receive TC messages from the nodes 13 or 14. Thus, the additional load caused by these two critical MPRs is much smaller than that of the nodes 4 and 7. Hence the different predicted maxium loads.

VI. Conclusion

The results show, that our predictions can be used to precisely estimate the incoming load caused by OLSR control messages for an arbitrary node, with only the node positions and their communication ranges as an input. Though the formulas presented in this work are designed to estimate the TC message load, they can easily be adapted to any MPR flooded messages emitted in regular intervals. Instead of predicting the incoming packet sizes it is also possible to estimate the number of incoming packets with only little modifications.

Computing the estimated load using our predictions is at least one order of magnitude faster than running detailed simulations. Therefore, it is possible to evaluate the effects of different TC intervals on protocol overhead in a timely manner.

The formulas neither account for propagation delay nor node mobility nor packet losses due to fading and collisions. To use them with more sophisticated propagation loss models or real world deployments, additional link characteristics have to be considered. Current work focuses on extending our predictions to include packet delivery probabilities for all links.

References

[1] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, Oct. 2003.

[2] C. Gomez, D. Garcia, and J. Paradells, "Improving performance of a real ad-hoc network by tuning OLSR parameters," in *Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on*, Jun. 2005, pp. 16 – 21.

[3] D. Nguyen and P. Minet, "Scalability of the OLSR Protocol with the Fish Eye Extension," in *Networking, 2007. ICN '07. Sixth International Conference on*, Apr. 2007, p. 88.

[4] W. Jiang, Y. Zhu, and Z. Zhang, "Routing Overhead Minimization in Large-Scale Wireless Mesh Networks," in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, Apr. 2007, pp. 1270 –1274.

[5] P. Jacquet, A. Laouiti, P. Minet, and L. Viennot, "Performance of Multipoint Relaying in Ad Hoc Mobile Routing Protocols," in *Proceedings of the Second International IFIP-TC6 Networking Conference on Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; and Mobile and Wireless Communications*, ser. NETWORKING '02, 2002, pp. 387–398.

[6] A. Medina and S. Bohacek, "Performance model of flooding in OLSR," in *Proceedings of the 7th ACM workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, ser. PE-WASUN '10, 2010, pp. 58–65.

[7] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, ser. MobiCom '99, 1999, pp. 151–162.

[8] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, Jan. 2002, pp. 3866 – 3875.

[9] "ns-3," Nov. 2012. [Online]. Available: http://www.nsnam.org/

[10] E. Kohler, "The Click Modular Router Project," Nov. 2012. [Online]. Available: http://read.cs.ucla.edu/click/click

[11] A. Jayasuriya, S. Perreau, A. Dadej, and S. Gordon, "Hidden vs. Exposed Terminal Problem in Ad hoc Networks," in *Proceedings of the Australian Telecommunication Networks and Applications Conference Sydney Australia*, 2004.

Face-to-Face Ad-hoc Networking on Android

Marcel Großmann, Lukas A. Schwöbel, Udo R. Krieger
Faculty of Information Systems and Applied Computer Science
Otto-Friedrich University
Bamberg, Germany
{marcel.grossmann, udo.krieger}@uni-bamberg.de
lukas-antii.schwoebel@stud.uni-bamberg.de

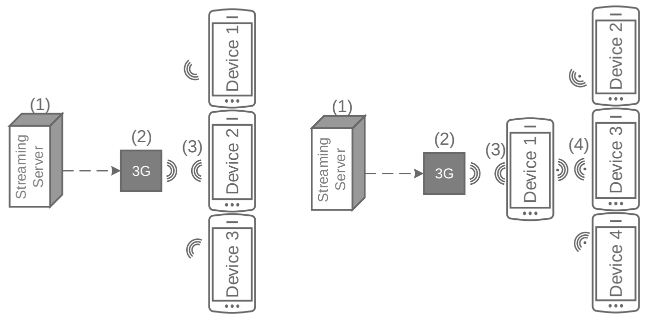
***Abstract*—Mobile data consumption establishes as a massively growing market, because the proliferation of powerful smartphones and tablets on mobile networks is a major traffic generator nowadays. Those devices offer content and applications to the consumer that were not supported by previous generations of mobile devices. In order to guarantee an acceptable quality of experience to the end user, current studies try to improve data transmissions on air interfaces. However, the bottleneck in cellular mobile networks is the traversal of the infrastructure. A paradigm to circumvent this fact and to increase the system's capacity is given by face-to-face communication in combination with proximity detection. Those networks promise scalability and performance improvements in utilizing scarce resources. Without using new hardware, a face-to-face paradigm is implemented and tested with a chat application for the Android operating system. It is based on a methodology to discover devices that are in near distance to each other. Finally, a measurement trial reveals the battery drainage of smart devices in self established ad-hoc networks.**

I. Introduction

Among a few other scientific studies on mobile peer-to-peer (P2P) video streaming, Eittenberger *et al.* [1] present a prototype for a mobile P2P video streaming application running on the Android operating system (OS). The bottleneck for the video streaming of the framework and similar P2P networks is their current restriction to rely on the existing mobile network infrastructure. The connections to a P2P network, which mobile devices can establish, are mostly twofold: On the one hand, a mobile handheld can connect via an IEEE 802.11 wireless network, if the smart device provides the corresponding hardware. The WiFi infrastructure is used for short distances, dedicated to an area with static access points (AP), and offers a limited mobility to the smart device. On the other hand, cellular air interfaces are providing another entry point to the Internet. The performance of the second type of infrastructure is barely achieving the requirements for participating in the P2P data dissemination and is by far smaller than in the WiFi setup. Nevertheless, it provides the maximal mobility to the user of a smart device. Additionally, a cellular network over relatively narrow air interfaces suffers from hand-overs between the base stations (BS), which are handled by radio network controllers (RNC), and areas that are not covered by a BS. Hua *et al.* [2] propose a multicast approach with ad-hoc transmissions. In their study the video is encoded into different layers, one base layer and multiple enhancement layers. Thus, devices with a higher distance from the BS receive less enhancement layers. If there are a few more peers between the BS and the receiver, the proposed ad-hoc multicast extension allows the reception of layers with a higher quality for devices that are farer away.

Moreover, a mobile device is able to participate in a P2P data dissemination paradigm in a few more ways. Since most smart devices provide the ability to open an IEEE 802.11 AP, a proximity based approach for P2P networks is possible, such that *face-to-face* (F2F) connections can be used for data transmission. However, this paradigm should be analyzed further to consider the battery drainage of mobile devices. Obviously, it is higher if a mobile device opens two connections over different interfaces concurrently. Here, smart algorithms must be invented to create an incentive for devices that have a relatively high amount of energy to offer it voluntarily to other devices and in this way support the P2P network. Of course, proximity based network establishment is only useful, if a crowd of peers, which are in near distance to each other, participate in the F2F network. Luckily, nearly every smart mobile device provides a GPS sensor that can be used to determine the actual position of a peer.

The scenario of mobile P2P video streaming is an useful example, while there are crowds that watch, e.g., sport events at the same place and time. The results generated in this scenario are fundamental to develop applications for current and upcoming mobile devices that are capable for standards proposed by the



(a) Traditional transmission (b) F2F enhanced transmission

Fig. 1. Data dissemination strategies compared. A video streaming server transmits its media content via a 3G network to requesting devices.

3GPP Long Term Evolution (LTE) group. Upcoming approaches to use F2F communication on the physical layer are, for example, FlashLinQ [3] by Qualcomm or the LTE advanced approach presented by Fodor *et al.* [4] that describe methods to increase the spectrum and energy efficiency of traditional cellular networks.

We provide a first implementation of a chat application prototype that uses a F2F overlay for the exchange of messages. It is based upon the communication principle to connect nearby devices directly and thus, data transmissions are possible without further infrastructure. The prototypical implementation of a F2F chat lays the foundation to evaluate such a transmission paradigm.

II. Data Dissemination in Next Generation Networks

A. *Face-to-Face Transmission*

We assume that several devices trying to establish connections at the same time in the same cell are really near to each other. Figure 1 reveals two different data dissemination scenarios. While Figure 1a depicts the *traditional* data transmission with a BS (2) and non intelligent devices, Figure 1b shows a transmission paradigm, where one device (3) acts as an AP for a group of devices. Through the AP all connected devices communicate F2F without the need of a mobile network infrastructure.

Figure 2 shows a simplified diagram of the developed Android activity stack and the communication paradigm between the activities. The *Application* stores information, e.g., the WiFi IP address, the location of the tracker-server, an identifier for the device in the F2F overlay and some device specific data. The F2F communication paradigm itself consists of two phases that are derived from the Android *Activity* class. In the first phase, the application starts the *BootstrapActivity*, which is responsible for the initialization of the application. It gathers information about the device and estimates the device's geolocation as described in Subsection II-B. The data is frequently sent to a tracker-server, which evaluates them and determines, if there are devices nearby to construct a WiFi F2F overlay. During this phase, either a WiFi AP is opened or the device connects to an already existing WiFi AP that is in near distance to the current device. Therefore, the tracker-server requests the device with the highest battery charge to open an AP and informs all nearby devices, how to establish the connection to the WiFi network.

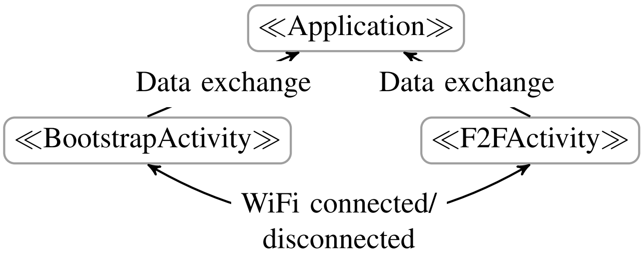


Fig. 2. Android activity stack for establishing a F2F overlay. The Application first launches the *BootstrapActivity* to set up the WiFi connection. If the device is connected via WiFi, the *F2FActivity* starts and establishes the overlay. Is the WiFi disconnected, the *BootstrapActivity* continues.

Once a successful WiFi connection is established, this activity is stopped and remains in the background, while an instance of *F2FActivity*, the second phase, is started. Within the second activity, a F2F overlay is established that distributes data among the participating devices. To test the data exchange prototypically, the app starts a F2F chat. Furthermore, the synchronization with the tracker-server continues, such that the geolocation of the device is continuously updated. New activities in Android are per default started on top of others. There is only one foreground activity while the rest remains in the background. If the WiFi connection is lost or the user presses the *back* button, the *F2FActivity* instance is destroyed and the *BootstrapActivity* resumes, trying to find new matching APs again.

B. *Proximity Detection*

In order to obtain the device's location and to discover other nearby devices, several metrics need to be obtained. First, in the mobile context, the solution should be efficient and save battery charge. To achieve this and to guarantee a good user experience, locating the device should be fast. The longer a global positioning system (GPS) signal is received to get a better accuracy, the more battery power is consumed. If the accuracy is already good enough to identify nearby devices, there is

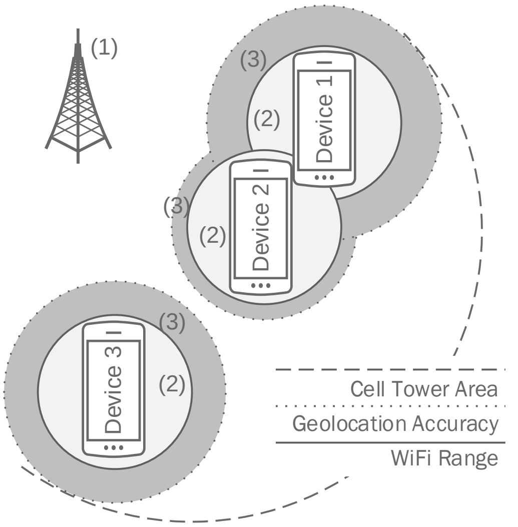


Fig. 3. There are several possibilities to obtain the geolocation of a device. As possible estimates for the location of a device the cell tower area is plotted in white with a dashed circle, the received GPS position and its accuracy in dark gray with a dotted circle and the WiFi range in light gray.

no need to consume more time and waste battery power for a better accuracy. Device location is performed in multiple steps with different accuracies. Figure 3 shows three different types of information that are used by the tracker-server to evaluate the device's location and nearby devices.

The cell tower (1) serves the devices with a mobile network connection like 3G. In Android it is possible to read the location area code (LAC) and the cell ID (CID). The geo-position of the cell tower is determined by using an API[1] from Google. The big dashed circle represents the accuracy of this method. As only the location of the cell tower is obtained but not the device's location, the obtained position is only as good as the size of the cell. Unfortunately, there seems to be no way to obtain the size of a cell and an accuracy of 1,000 meters is assumed. Of course, this is not precise but has some advantages. If the device is inside a building there is no way to get a GPS signal, but the CID can still be obtained as long as there exists a mobile network connection. Also, the position of the cell tower is determined instantly and without noteworthy additional battery consumption. Thus, we consider it as an appropriate backup alternative for the geolocation.

As there is only a limited amount of time when the GPS position will be obtained, this position will not be accurate as well. The dotted circles (3) show the corresponding accuracy of the received GPS positions for the devices. The current approach at the tracker-server is to use this accuracy values in order to find nearby devices. Devices that are within the dotted radius of the dotted circle are assumed to be nearby. Finally, the critical point is the reachable area of the device's WiFi (2). If the circles of two devices are overlapping, they are considered to be within each others WiFi coverage. As explained before, the tracker-server is not able to get the exact position of a device because the position is not accurate enough. Obviously, the obtained accuracy of the GPS location of *Device 1* in Figure 3 is not very good. If the device would be positioned a bit more in the north, it would not be in the WiFi coverage area of device *Device 2*, though it is still considered as a nearby device, because the transmitted inaccurate positions are overlapping. Even worse is *Device 3*, which is nowhere near other devices but still in the same network cell. If this device only transmits its cell location (with a presumed accuracy of 1,000 meters), the tracker-server determines that it is within the network coverage of the other devices in the same cell. However, there would be no harm if the tracker-server makes false assumptions based on too inaccurate geolocations. The worst that happens is that one device opens up a WiFi AP without another device really being able to connect. Thereafter, the protocol waits for the first device to connect and remains in an idle state. The remaining devices would continue searching for an open AP. It only consumes and wastes more battery power at the device with the open AP.

Though the F2F approach is possible, we need to consider the WiFi signal propagation to improve the overlay specifications. Moreover, we try to estimate the battery consumption generated by the data transmissions within the F2F overlay network.

III. WiFi vs. Battery Drainage

A. Signal Strength

We have obtained the received signal strength indicator (RSSI) on a Huawei Mediapad (running Android 4.0) as AP. In addition, a laptop served as monitor while it captures WiFi beacons with the help of *aircrack-ng* [5] and *tcpdump* [6] on its wireless interface. The monitor observed the broadcast beacons of the AP and was moved in steps of 5 meters away from the AP in line of sight for several times. For each distinct distance 1,000 broadcast beacons of the collected traces have been analyzed, particularly the field from the radiotap header of each beacon that contains the RSSI value. In Figure 4 the mean values of the RSSIs and their 95% confidence levels are plotted. We observe a relatively

[1] http://www.google.com/glm/mmap?mcc=xxx&mnc=xxx&towerid=xxx

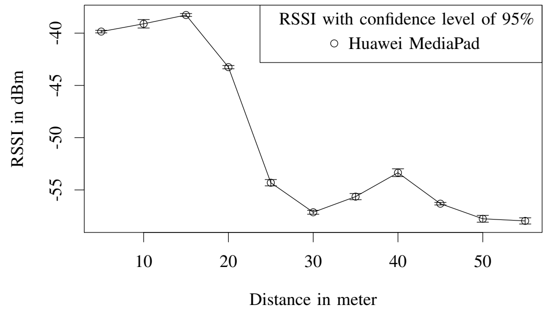


Fig. 4. The mean of the RSSI values with a confidence level of 95% monitored on several distances. While the Android device opens the AP, a monitor device was moved in steps of 5 meters away from it.

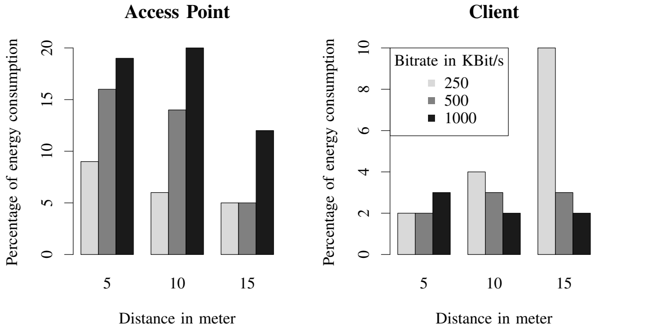


Fig. 5. Percentage of energy consumption for transmitting date from the client to the AP. The bars are plotted for several distances (5, 10 and 15 meters) and different bitrates (250, 500 and 1,000 $\frac{\text{KBit}}{\text{s}}$).

high RSSI value up to 20 meters, followed by a rapid decrease. According to this observations, we analyzed the battery drainage of random data transmissions with an increasing distance of up to 15 meters in Subsection III-B. Additionally, we observed that presumably some constructive interference increases the RSSI value at around 40 meters, before it continues to decrease slightly again.

B. Battery Drainage

We determined the battery drainage of two devices, the Huawei U8160 with Android 2.2 as AP and the Huawei Mediapad with Android 4.0 as client counter part. The measurement setup contained different settings with alternating bitrates and distances between the devices. Therefore, random traffic is sent from the AP to the client side in three different rates for a total time of ten minutes. In the measurements three different distances, 5, 10 and 15 meter were observed with traffic rates of 250, 500 and 1,000 $\frac{\text{KBit}}{\text{s}}$. Figure 5 depicts the percentage of the battery drainage, on the left side for the device that opens the AP and on the right side for the connected client. The total battery consumption on the client side increases for 250 and 500 $\frac{\text{KBit}}{\text{s}}$ for higher distances, but decreases for transmissions with 1,000 $\frac{\text{KBit}}{\text{s}}$. This behavior could be caused by an energy scheduling algorithm of the Android framework, but needs to be further investigated on devices running different Android versions. In contrast, the AP generally shows a decrease of the consumption by an increasing distance and a lower bitrate.

IV. Conclusion & Future Research

The developed prototype lays the foundation to evaluate a new F2F transmission paradigm, especially concerning the battery drainage of mobile devices. Moreover, it contains a strategy to find nearby located devices in an appropriate manner. Of course, there is plenty of room to implement new ideas, e.g., a beaconing process to find nearby devices without the need of a central controller instance. In addition, the measurement of the battery power consumption revealed a varying behavior of devices that opened an AP compared to the client counter part. Future research concerning power wastage should consider the influence factors for this observation. With regard to the transmission of media content, this could be a feasible approach to offload mobile network infrastructures, especially by enhancing mobile P2P systems with a F2F approach.

Acknowledgment

The authors would like to thank Dr. Ingo Dahm of the Deutsche Telekom AG for the provided access to the T-Mobile 3G network.

References

[1] P. Eittenberger, M. Herbst, and U. Krieger, "RapidStream: P2P Streaming on Android," in *19th International Packet Video Workshop (PV 2012), Munich, Germany, 10-11 May 2012*, 2012.

[2] S. Hua, Y. Guo, Y. Liu, H. Liu, and S. S. Panwar, "Scalable Video Multicast in Hybrid 3G/Ad-hoc Networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1–6.

[3] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia, and A. Jovicic, "FlashlinQ: a synchronous distributed scheduler for peer-to-peer ad hoc networks," in *Communication, Control, and Computing (Allerton), 2010 48th Annual Allerton Conference on*, 2010, pp. 514–521.

[4] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Mikls, and Z. Turnyi, "Design aspects of network assisted device-to-device communications," *Communications Magazine, IEEE*, vol. 50, no. 3, p. 170177, 2012. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6163598

[5] "Aircrack-ng." [Online]. Available: http://www.aircrack-ng.org/

[6] "Tcpdump." [Online]. Available: http://www.tcpdump.org/

A Security Extension for Ad-hoc Routing Protocols

Peter Racz, Andrew Lunn, Janne Paatero
RUAG Schweiz AG, Switzerland
{peter.racz|andrew.lunn|janne.paatero}@ruag.com

***Abstract* — Ad-hoc networks provide communication services in scenarios where no infrastructure is available. They require special routing protocols that can adapt to fast changing topology and link quality. Existing ad-hoc routing protocols focus on fast convergence and efficient packet forwarding. However, they typically communicate in plain text and are vulnerable against various attacks that can seriously compromise ad-hoc networks. Therefore, in this paper we propose a security extension working on layer 2 which is applicable to multiple ad-hoc routing protocols. It provides integrity, confidentiality and replay protection for routing messages and user traffic. It has been implemented in Linux and tested in a network test bed. It enables flexible prototyping of different security mechanisms and provides the basis for the development of a secure ad-hoc network.**

I. Introduction

Ad-hoc networks are especially suitable for providing network services in situation where no existing network infrastructure is available. Typical application scenarios include natural disasters, rescue and military operations. In an ad-hoc network every node acts as a router and forwards packets to other nodes. To cope with the special requirements in ad-hoc networks, like fast convergence time after topology changes and efficient use of network resources, new routing protocols have been developed, like Ad-hoc On-Demand Distance Vector (AODV) routing [9], Optimized Link State Routing (OLSR) [3], Better Approach To Mobile Ad-hoc Networking (BATMAN) [1], and Babel [2].

The ad-hoc network environment imposes also new security threats to routing protocols. Besides typical security threats on network traffic, like eavesdropping or replay attacks, ad-hoc networks are also vulnerable to attacks targeting the routing protocol. Many attacks, like wormhole, blackhole and flooding attacks [7], are known against routing protocols that can seriously affect the network and disrupt network services. Despite this, ad-hoc routing protocols often exchange messages in plaintext and do not include any security mechanism. It is often expected to use such protocols with lower-layer security mechanisms. Furthermore, there is a difference in crypto support in hardware for wireless and wired networks. While wireless LAN cards have crypto support in hardware, Ethernet cards do not. Thus, if a protocol is meant to be used in a scenario with wireless and wired links, it is usually not possible to have all security mechanisms in hardware.

Therefore, in this paper we propose a software-based security extension that works below the routing protocol on layer 2 and is applicable to several ad-hoc routing protocols. It enables flexible prototyping and developing new security mechanisms. Since the solution is mesh technology agnostic, the routing protocol can be easily exchanged or updated. The security extension uses standard Linux modules and tools, which reduces the implementation effort.

In this paper we have selected BATMAN as the routing protocol and present SecBATMAN, the security-extended version of the protocol. BATMAN is a proactive routing protocol and works in a distance vector manner. Neighbors, nodes that are in the range of a given wireless technology, continuously monitor their link quality. According to this metric they calculate the best next hop. The protocol can cope with asymmetric links that are usual in wireless networks. It also supports the interconnection to non-BATMAN networks via gateway nodes that can announce themselves in the ad-hoc network. The routing protocol is part of the official Linux kernel.

SecBATMAN provides hop-by-hop security based on a shared symmetric session key between neighbors. It can be applied with different levels of security and to various traffic types. It can provide either message authentication and integrity protection or additionally message confidentiality. SecBATMAN can protect either routing messages only or protect both routing and user traffic depending on the security level required and the processing resources of network nodes. Furthermore, different crypto algorithms can be used as well. The session key can be configured manually on all nodes or dynamically negotiated, enabling a frequent renewal of keys. In this paper we focus on the secure communication between neighbors and key negotiation is not discussed in detail. The mechanism has been implemented and tested in an ad-hoc network test bed, demonstrating the feasibility of the approach.

II. Secure BATMAN

The key goal of SecBATMAN is to protect the routing protocol against malicious injection of invalid routing information and to protect the network against unauthorized access. Requirements for SecBATMAN include message authentication, integrity, confidentiality, and replay protection. Additionally, it shall provide efficient use of network resources and impose low overhead.

BATMAN operates on layer 2 and it includes an additional layer between the data link and IP layers. It encapsulates layer 2 frames and forwards them until they reach their destinations. BATMAN routing is transparent to the IP layer. Thus, security mechanisms applied on top of BATMAN (like IPSec or end-to-end security on the application layer) are not sufficient, as these are not able to protect the ad-hoc network itself. Therefore, SecBATMAN includes security mechanisms below the BATMAN protocol as illustrated in Fig. 1.

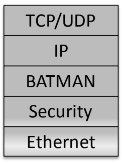


Fig. 1. Protocol stack

We assume that in a single mesh network all nodes use the same security mechanisms and are configured with the same crypto algorithms. SecBATMAN encapsulates all BATMAN packets and inserts a new security header into all frames. The new frame format is shown in Fig. 2. SecBATMAN can apply message authentication only or encryption as well. Accordingly, the frame can include different fields. In the following we always assume the use of both to ease the description. The SecBATMAN header is inserted after the original Ethernet header with the source and destination addresses. The new Ethernet frame type 0x4306 signals that the frame is a SecBATMAN frame. The header contains the initialization vector used by the encryption algorithm and the message authentication code. The SecBATMAN header is followed by the original BATMAN packet. An optional padding closes the frame whose length is included in the padding length field. The padding extends the frame size to the block size of the block cipher algorithm. The authentication hash is calculated over the complete frame, excluding the hash itself. The encryption covers the complete original BATMAN packet, the padding length and the padding.

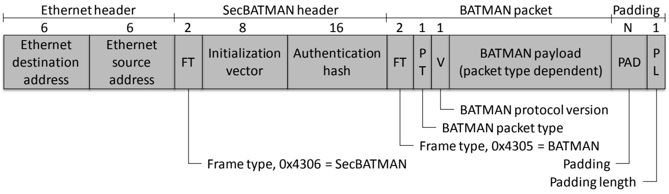


Fig. 2. SecBATMAN frame format

The concept of SecBATMAN and the usage of crypto keys are illustrated in Fig. 3 for an example network consisting of three nodes (A, B, C) and a malicious node (M). Each node with its direct neighbors represents a neighbor group. In the example A with B, B with A and C, and C with B. Since wireless networks are typically a broadcast medium, SecBATMAN does not use separate pairwise keys per peer but each node uses its single session key to send packets to all its neighbors. Sending broadcast frames with a pair-wise key would mean too much overhead in a broadcast medium since each frame would have to be encrypted and sent separately to each neighbor. Depending on the number of neighbors, this would waste bandwidth resources and reduce the total throughput in the network. Furthermore, BATMAN frequently sends broadcast messages to measure the link quality.

As shown in Fig. 3, SecBATMAN uses a hop-by-hop protection between nodes. Each node has its own session key for sending and a key table with the MAC address–session key pairs for all other nodes, e.g., on node A the session key is SK_A and the key table contains B – SK_B and C – SK_C. When a node sends a packet (either from a local process or forwarding a packet from another node), it encrypts the message with its session key and sends it to the next hop in the ad-hoc network. For example node B encrypts message M_B with SK_B and send $\{M_B\}_{SKB}$. Because of the wireless medium, the message can be received by any node within transmission range. But only nodes that possess key SK_B can decrypt and further process the message. The malicious node M cannot decrypt it. Similarly, if the malicious node M tries to inject packets into the network, it sends a message $\{M_M\}_{SKM}$ using its self-generated key SK_M. The message can be received by B and C, but it will be dropped because it comes from an unknown MAC address. Even if M spoofs another node, using the MAC address of node A for example, the message authentication will fail on nodes B and C, since M does not know SK_A. Thus, SecBATMAN ensures that a node accepts packets only from nodes that belong to the ad-hoc network. Packets from other nodes will be dropped and will not be forwarded.

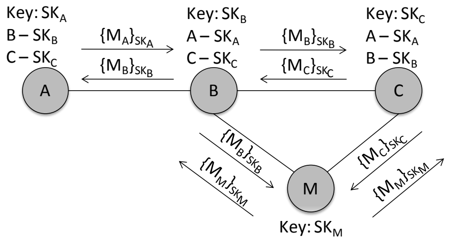


Fig. 3. Session keys and message encryptions in an example network

We assume here the manual configuration of static keys on all nodes belonging to a single ad-hoc network. However, the keying scheme allows dynamic key generation locally on each node as well as rekeying during operation. Rekeying affects only neighbors and does not have to be propagated through the whole network.

III. IMPLEMENTATION

SecBATMAN has been implemented in Linux using kernel 3.3.0 and batman-adv of version 2012.0.0 [1]. The security extensions have been integrated using the bridging support and the ebtables filtering tool [5] of the Linux kernel. The implementation architecture is shown in Fig. 4. The network device driver provides the access to the network via the `wlan0` interface. The bridging module creates the new interface `br0` and bridges it to `wlan0`. The BATMAN kernel module implements the routing protocol and provides the `bat0` interface on top of `br0`. The `bat0` interface is configured with an IP address on all nodes and it is used by all applications running on a node. The bridging module enables the use of the general filtering and frame processing features of ebtables by passing all frames through the ebtables kernel module. We have implemented new ebtables targets (`encrypt`, `decrypt`) that use the crypto algorithms of the kernel and can be used in the filtering rules to perform the message authentication and encryption. The `ebtables` user space program is used to configure filtering rules and to set session keys.

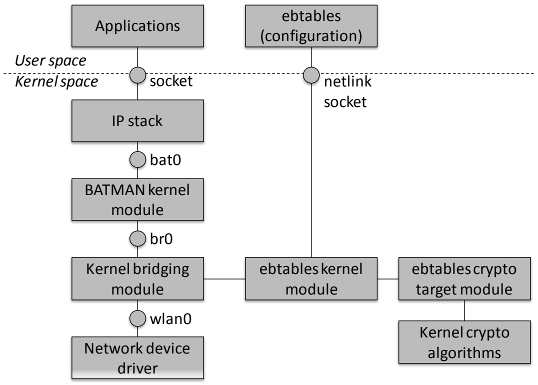


Fig. 4. Implementation architecture

The implementation uses the crypto algorithm Advanced Encryption Standard (AES) [8] in Galois Counter Mode (GCM) [4] of the Linux kernel. AES-GCM is an efficient and high-performance symmetric key block cipher algorithm that provides message authentication, integrity and confidentiality. AES-GCM is used with a key length of 128 bits. Fig. 5 shows the ebtables rules on a node with one peer only. The input chain forwards all frames coming from the peer to a separate input chain and drops any other packets (policy drop). The output chain drops any non-BATMAN packets (`!0x4305`) and encrypts all remaining BATMAN packets using the new `encrypt` target. The encryption key and salt are stored in separate files with appropriate access rights. The key and salt are set by passing the file names to ebtables in the `encrypt-key` and `encrypt-salt` parameters. In general there is a separate input chain for each peer identified by its MAC address. The input chain of the peer drops all non-SecBATMAN (`!0x4306`) packets, decrypts the packets using the new `decrypt` target and accepts them if they are authenticated.

```
Bridge chain: INPUT, entries: 2, policy: DROP
-s 0:80:48:6b:9d:58 -i wlan0 -j INPUT_00:80:48:6b:9d:58

Bridge chain: FORWARD, entries: 0, policy: ACCEPT

Bridge chain: OUTPUT, entries: 3, policy: ACCEPT
-p ! 0x4305 -o wlan0 -j DROP
-o wlan0 -j encrypt --encrypt-key /etc/... --encrypt-salt /etc/...

Bridge chain: INPUT_00:80:48:6b:9d:58, entries: 3, policy: DROP
-p ! 0x4306 -i wlan0 -j DROP
-i wlan0 -j decrypt --decrypt-key /etc/... --decrypt-salt /etc/...
-i wlan0 -j ACCEPT
```

Fig. 5. Status of ebtables on a node with one peer

The SecBATMAN overhead, i.e. the additional bytes per frame, is 2 bytes for the frame type, 8 bytes for the initialization vector, 16 bytes for the authentication hash, 1 byte for the padding length and 0-3 bytes for the padding. Thus, it is 27-30 bytes in total. First measurements in a WLAN-based ad-hoc network show that SecBATMAN can achieve around the same throughput as BATMAN (around 16Mbps in our setup). The CPU load approximately doubles for sending and receiving packets with SecBATMAN on a system with an Intel Atom N270 1.60GHz CPU.

IV. CONCLUSION AND FUTURE WORK

SecBATMAN supports message authentication, integrity and confidentiality for routing messages and user traffic by encapsulating all BATMAN frames. It ensures that only authorized nodes can participate in the ad-hoc network and malicious nodes are excluded. It provides the basis for a secure ad-hoc network using the BATMAN routing protocol. Our implementation is based on existing tools and modules of the Linux operating system. It uses the built-in crypto algorithms of the kernel and extends the ebtables tool with encryption and decryption using AES-GCM. The security extension works on layer 2 and is applicable to multiple routing protocols. First measurements show that SecBATMAN is feasible and provides appropriate performance. The concept of session keys fits especially to the broadcast nature of wireless networks, so that it imposes minimal overhead.

In this paper we assumed manually configured static keys on all nodes. However, we are currently working on the dynamic generation and negotiation of session keys between neighbors. We are extending the presented solution with neighbor authentication and attestation based on trusted computing mechanisms, which will allow for automatic rekeying. Additional future work includes further measurements and the use of hardware support for crypto operations. We plan to have a hybrid solution making use of the hardware acceleration of the wireless chip, but retaining the key scheme and software based crypto for network technologies without available crypto hardware. The software based solution could also benefit from the Intel AES New Instructions (AES-NI) [6] resulting in higher performance and/or lower system load.

V. ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7-ICT-2009.1.4) under grant agreement n° 256668. The authors would like to thank all SecFutur project partners for their collaboration and inspiring discussions and insights.

REFERENCES

[1] BATMAN project website, http://www.open-mesh.org/, Nov. 2012.

[2] J. Chroboczek, "The Babel Routing Protocol", IETF RFC 6126, April 2011.

[3] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, Oct. 2003.

[4] M. Dworkin, "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf, Nov. 2007.

[5] Ebtables project website, http://ebtables.sourceforge.net/, Nov. 2012.

[6] A. Hoban, "Using Intel® AES New Instructions and PCLMULQDQ to Significantly Improve IPSec Performance on Linux", Intel White Paper, 324238-001, Aug. 2010.

[7] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", Wireless Communication, 14(5), 2007.

[8] NIST, FIPS PUB 197, "Advanced Encryption Standard (AES)", http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Nov. 2001.

[9] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF RFC 3561, Jul. 2003.

A New Security Mechanism for Ad-hoc On-demand Distance Vector in Mobile Ad Hoc Social Networks

Mohamed Amine FERRAG
University of Badji Mokhtar - Annaba, ALGERIA
Faculty of Science Engineering
Department of Computer Science
Laboratory Network and System "LRS"
E-mail: mohamed.amine.ferrag@gmail.com

Mehdi Nafa
University of Badji Mokhtar - Annaba, ALGERIA
Faculty of Science Engineering
Department of Computer Science
Laboratory Network and System "LRS"
E-mail: mehdi.nafa@gmail.com

Salim GHANMI
University of Badji Mokhtar - Annaba, ALGERIA
Faculty of Science Engineering
Department of Computer Science
E-mail: ghanemisalim@yahoo.com

***Abstract*— Routing is a primary function in Mobile Ad Hoc Social Networks. This is the mechanism by which the paths are created for routing data to the right destination through the social network. These routing protocols designed as lack of security controls, which increases the risk of attacks that can be orchestrated by external or internal nodes taking into account the position of the striker from the social network. In this paper, first, we analyze the vulnerability of AODV routing protocol. Second, we introduce a new system, called AODV-MASN. Third, we introduce a new security mechanism for this new system.**

Keywords—Ad Hoc Social Networks, AODV, Security, Routing Protocol.

I. INTRODUCTION

An Ad Hoc network is a wireless network with no fixed infrastructure in which all nodes participate in the routing. Ad hoc networks are considered particularly important in situations where the installation of a fixed infrastructure is costly, difficult, impossible or simply unnecessary.

The Ad Hoc routing protocols existing in the literature currently being standardized within the IETF (Internet Engineering Task Force) hypothesize an ideal environment in which the operation of the network is not under attack malicious about service availability and data integrity. They also assume that all nodes voluntarily participate in the operation of the network regardless of their natural tendency to abstain in order to save energy in their battery.

Securing the ad hoc routing is particularly difficult due to the lack of administrative entity in the heart of the network. There is much vulnerability allowing malicious nodes corrupt the configuration of routing tables, modify packets in transit or simply not participate in the effort routing in order to save energy. For this reason, the subject of this article focuses on the security of routing protocols. We have chosen the AODV [1] [2] routing protocol because it is the most widely used in ad hoc community. In the next section, we present brief attacks against MASN using AODV as routing protocol. We use the abbreviation MASN for "Mobile Ad Hoc Social Networks".

II. ATTACKS AGAINST MASN USING AODV AS ROUTING PROTOCOL

Many researchers address problems related to online social network in [12] [13]. Contrary to our type of social network that is completely mobile devices. In [15], we applied a part of this method for the OLSR routing protocol. Taxonomy of attacks against MASN is divided into two classes: external and internal attacks. External attacks nodes that are not part of the network. Internal attacks nodes are a legitimate part of the network. We present in Table 1 the various attacks which exist in the literature.

III. A NEW SECURITY MECHANISM FOR REACTIVE ROUTING PROTOCOL AODV IN MASN

In this section, we introduce a new system "AODV-MASN" then we describe our new security mechanism to AODV protocol in MASN. In our approach, nodes first try to detect suspicious links before the route request.

A. *Overview of "MASN with AODV"*

MASN with AODV is shown in Fig 1. Consists of two layers: (a) a physical layer of ad hoc network and (b) a layer of virtual social network. In the network layer (virtual) social are connected by virtual links where AODV is used as routing protocol. Each virtual link is to a communication channel which may be composed of several hops. Once the friendly relations are established, friends can perform social such as resource sharing, sending messages, and navigation from each other.

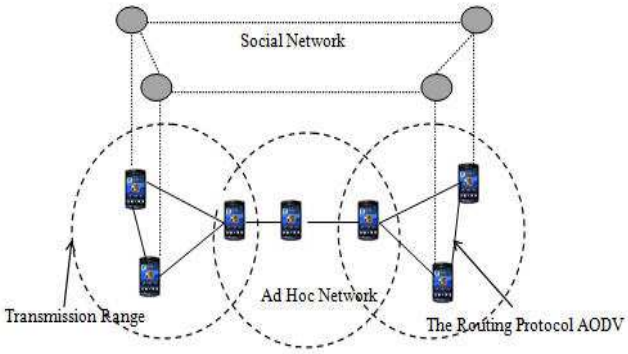
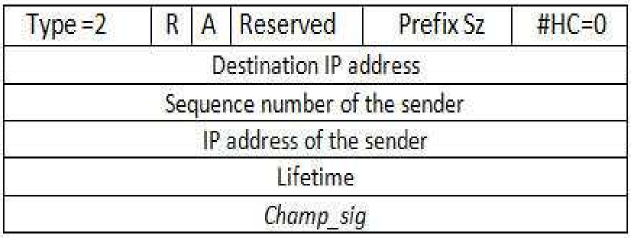


Fig 1. *Presentation of MASN with AODV*

b. *Detect of suspicious links in MASN with AODV*

The fig.2 represents our approach and our system parameters are presented in Table 2. Before the detection of suspicious links, the mobile nodes are changing their public key (Fig 2 Step 1) then he changed the secret keys with confidentiality and authentication (Fig2.Step 2)**.**



Type =2	R	A	Reserved	Prefix Sz	#HC=0
Destination IP address					
Sequence number of the sender					
IP address of the sender					
Lifetime					
Champ_sig					

Fig3. *Datagram Message DetectReq , DetectRep*

To infer suspicious links, we define two messages new control for AODV "*DetectReq* & *DetrectRep*" (Fig. 3), they have the same format of the HELLO message, but we added a field "*Champ_sig*" to detect suspicious links. When a source node wants to establish a route to a destination for which it does not yet have a way. Before it broadcasts a packet broadcast RREQ, a mobile node encrypts the field "*Champ_sig*" of message *DetectReq* and send it. When a mobile node receive *DetectReq*, it decrypts the field value "*Champ_sig*" and checks if this contains information about *DetectReq* at each of its requests, if there is no information about its previous requests, the mobile node addresses the *DetectReq* received as a normal Hello message else the node control the arrival time of received *DetectReq* and the arrival in the waiting period specified; the node performs the link between itself and the mobile node that sent the *DetectRep* as suspicious and stops communicating with this mobile node.

Parameter	**Description**
X1	Mobile node in the circle of transmission from node "X2"
X2	Mobile node in the circle of transmission from node "X1"
X3	Mobile node in the circle of transmission from node "X2"
KUX1	Public key of the node "X1" (available at "X2")
KUX2	Public key of the node "X2" (available at "X1")
KRX1	Private key of the node "X1" (known only as "X2")
KRX2	Private key of the node "X2" (known only as "X2")
DetectReq	Message to detect the attack
DetectRep	Message for acknowledge receipt of the message "*DetectReq*
RREQ	The polling message of available routes
REEP	The response message to the route request
DATA	-See friend's online (nodes in the network), - Remove a shared file, - Delete a received message…
RRER	The message indicating a route error.
EKUX1	Encrypted with the public key of the node "X1"
DKUX2	Decrypt with the public key of the node "X2"
EKRX1	Encrypted with the private key of the node "X1"
DKRX2	Decrypt with the private key of the node "X2"
B	*DetectReq* encrypted
D	*DetectReq* decrypted
C	*DetectRep* encrypted
A	*DetectRep* decrypted
DKUX1	Decrypt with the public key of the node "X1"
1	Distribution of public keys by annoncement public.
2	Secret key distribution with privacy and authentication
3	Detection of suspicious links
4	Establishment of the road
5	Transfer data on establishes the road
6	Return to the applicant indicating roads error
⊗	The link failure

Tab2. System parameters

IV. CONCLUSION

In this paper, first, we have provided the taxonomy of attacks and their influence on the security property in MASN using AODV as routing protocol. Next, we introduced a new social network, called AODV with MASN. At the end, we presented our new security mechanism based on the use of two messages "*DetectReq*, *DetectRep*" and digital signatures "*Champ_sig*" to detect malicious links.

Attacks	Influence on the security property				Target	Result
	Confidentiality	Authentication	Integrity	Availability		
Detour attack [3]			x		Nodes in the direct vicinity of the opponent	Not participate in routing
Black hole attack [5]			x		Nodes specific	Creating a tunnel and disrupt routing
Wormhole attack [14]			x		Subset of nodes close to the hole	Creating a tunnel and disrupt routing
Routing table poisoning [4]			x		Subset of node	Division of routing
Sybil attack [6]	x	x	x		Nodes specific	Create of multiple identities
Man-in-the-middle attack [7]	x	x	x		Nodes specific	Use impersonation
Rushing attack [8]			x		Nodes in the direct vicinity of the opponent	Attract traffic
Resource consumption [9]	x	x		x	All nodes	Weakening battery
Routing table overflow [10]				x	Nodes in the direct vicinity of the opponent	Overflow of routing table
Location disclosure [11]	x	x			Nodes forming the path to a destination	Discover the location of mobile nodes

Tab.1 *Summary of attacks in AODV with MASN*

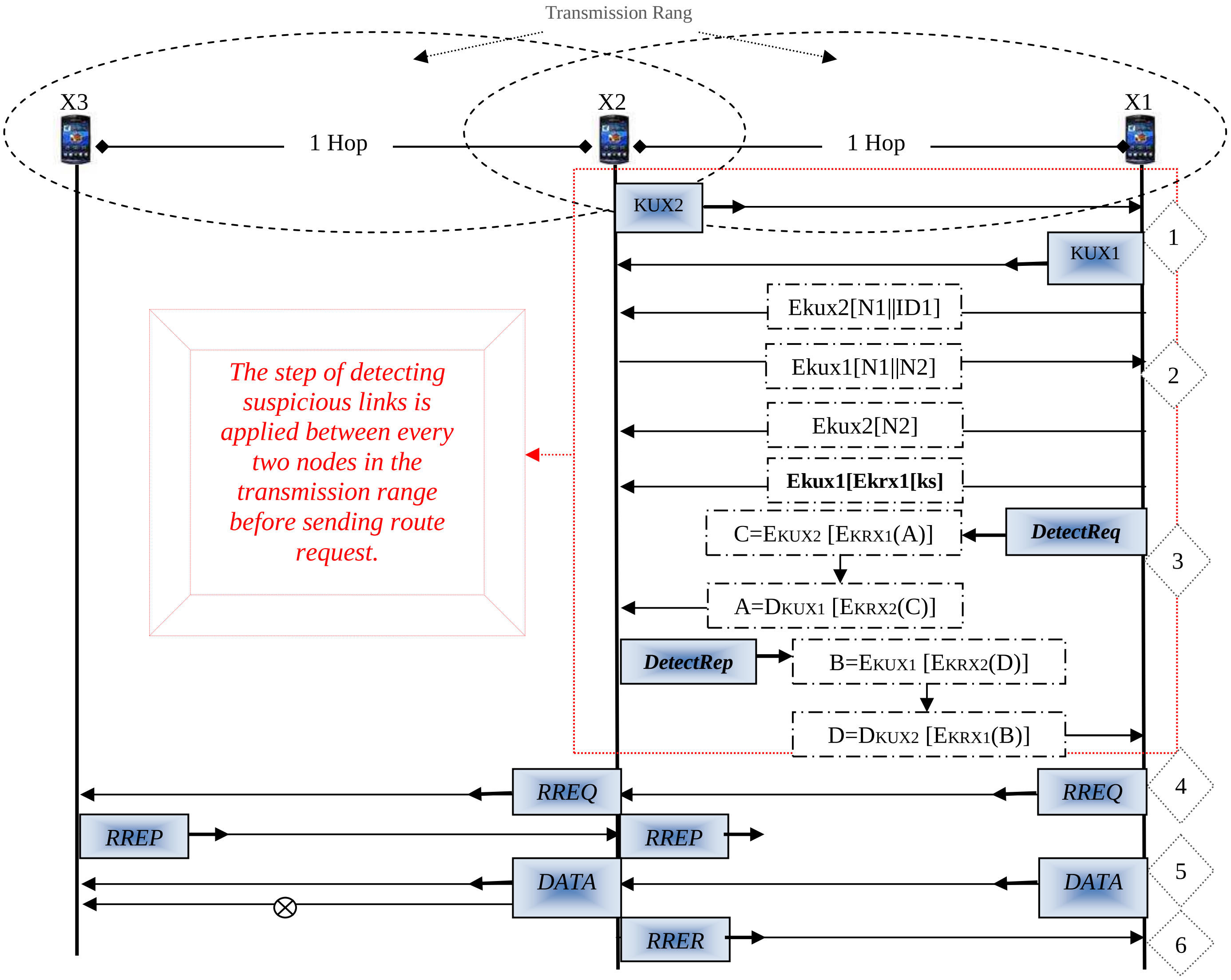


Fig .2 *Our New Security Mechanism for Ad-hoc On-demand Distance Vector*

REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. Http: //tools.ietf.org/html/rfc3561, July 2003. RFC3561.

[2] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings (WMCSA'99)*, volume 2, pages 90–100. IEEE Computer Society, February 1999.

[3] L. Guang, C. Assi, and A. Benslimane. Interlayer Attacks in Mobile Ad hoc Networks. In *Proc. of the Second International Conference on Mobile ad-hoc and sensor networks (MSN 2006)*, pages 436–448. Springer, December 2006.

[4] T. Condie, V. Kacholia, S. Sankararaman, J. Hellerstein, and P. Maniatis. Induced churn as shelter from routing-table poisoning. In *Proc. of the 13th Annual Network and Distributed System Security Symposium (NDSS'06)*, 2006.

[5] H. Deng, W. Li, and DP Agrawal. Routing security in wireless ad hoc networks. *IEEE Communications Magazine*, 40(10) :70–75, 2002.

[6] J. Douceur. The sybil attack. *Peer-to-Peer Systems*, 1 :251–260, 2002.

[7] C.Y. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. Levitt. A specification-based intrusion detection system for AODV. In *Proc. 1st ACM workshop on Security of ad hoc and sensor networks (SASN'03)*, pages 125–134. ACM, October 2003.

[8] Y.C. Hu, A. Perrig, and D.B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proc. of the 2nd ACM workshop on Wireless security*, page 40. ACM, 2003.

[9] I. Stamouli, P.G. Argyroudis, and H. Tewari. Real-time intrusion detection for ad hoc networks. In *Proc. Of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05)*, pages 374–380. IEEE Computer Society, 2005.

[10] S. Gupte and M. Singhal. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1) :151–174, 2003.

[11] G. Vigna, S. Gwalani, K. Srinivasan, EM Belding-Royer, and RA Kemmerer. An intrusion detection tool for AODV-based ad hoc wireless networks. In *Proc. of the 20th Annual Computer Security Applications Conference (ACSAC'04)*, pages 16–27. IEEE Computer Society, 2004.

[12] S. Guha , K. Tang , P. Francis, "NOYB: Privacy in Online Social Networks," Online Social Net., 2008, pp. 49–54.

[13] C.M.A. Yeung, et al., "Decentralization: The Future of Online Social Networking," Future Social Net., 2009.

[14] Y.C. Hu, A. Perrig, and DB Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2) :370–380, 2006.

[15] M.A. Ferrag , M. Nafaa , S. Ghanmi .OlsrBOOK: A Privacy-Preserving Mobile Social Network Leveraging on Securing the OLSR routing protocol. Proceeding of The 8 th International Scientific Conference eLearning and Software for Education . (2). 133-139, 2012.

Context-adaptive Networking for Ad-hoc Networks

Nils Aschenbruck
University of Osnabrück
Institute of Computer Science
aschenbruck@uos.de

Frank Kargl
University of Ulm
Institute of Distributed Systems
frank.kargl@uni-ulm.de

Björn Scheuermann
Humboldt University of Berlin
Department of Computer Science
scheuermann@informatik.hu-berlin.de

***Abstract*—Ad-hoc networks have been a topic in research for many years now. Over the time, different types of such networks like Mobile Ad-hoc Networks (MANETs), Vehicular Ad-hoc Networks (VANETs), Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), or Cyber-Phycial Systems (CPSs) have been proposed. In this paper, we point out that the common key challenge in these families of networks is the need to tailor them to application-specific requirements. In the past, this led to architectures which are hard or impossible to adapt to changing requirements and applications in the future. We argue that a context-adaptive network architecture with flexible per-application components in all network nodes can provide a solution.**

***Keywords*-Ad-hoc networks, Context-adaptive Networking**

I. Introduction

Ad-hoc networks are – by their very definition – networks that organize themselves in an independent and cooperative manner. In the first decade of the 21st century, there was a peak of research activity in this area. Since then, different terms were used to highlight and focus on certain properties. In fact, the following research areas can all be seen as specific incarnations of the idea of ad-hoc networking:

- Mobile Ad-hoc Networks (MANETs) [4] do not rely on infrastructure. The nodes can be mobile, and the networks are self-organizing. Typical usage scenarios are public safety or disaster recovery settings.
- Vehicular Ad-hoc Networks (VANETs) [6] focus on scenarios in which the mobile nodes are vehicles. Usage scenarios include those traffic safety, traffic efficiency, and convenience applications that require a direct and low-delay information exchange between cars without access to infrastructure.
- Wireless Sensor Networks (WSNs) [1] focus on sensor nodes that primarily monitor physical or environmental properties, and deliver the obtained data to one or few sinks. These nodes are often very resource constrained. Typical usage scenarios are monitoring such as wildlife monitoring or structural health monitoring.
- Wireless Mesh Networks (WMNs) [2] do also have meshed backbone, but in contrast to the networks mentioned before the backbone nodes are normally static. They form a self-organizing and self-healing infrastructure to provide other nodes with flexible backbone network access. Typical usage scenarios are community networks.
- Opportunistic networks [3] are networks that are frequently disconnected. An end-to-end path does typically not exist. Messages are ferried by the movement of the nodes, implying delay tolerance. Typical usage scenarios include network connectivity for rural and developing areas.
- Cyber-Phycial Systems (CPSs) are systems with sensors and actuators, which include feedback loops crossing the boundaries between the physical world and information processing systems. Ad-hoc networking concepts are inherent in CPSs whenever information exchange happens between multiple participating sensor or control devices. Typical usage scenarios are smart grid, smart factories, e-health, smart mobility, etc. (cf. [5]).

In the next section (Section II), we will discuss commonalities as well as differences of the specific incarnations and, finally, propose the concept of *Context-adaptive Networks*. After that (Section III), we consider a number typical ad-hoc networking scenarios and point out where they require application-specific functionality within the network. Subsequently (Section IV), we discuss the resulting challenges for pursuing a context-adaptive networking approach.

II. Context-adaptive Networking

What distinguishes the above mentioned network concepts from each other? In fact, the key ideas show substantial overlap in more than one regard. Depending on the specific application and setting, boundaries blur—for instance, between VANETs, CPSs, WSNs, and opportunistic networks. Self-configuration, interaction with the physical environment, resource constraints, and bandwidth constraints all apply to a certain degree. Despite those similarities, a look at the past decade's research suggests a necessity to re-design key building blocks for each of these areas. Most technical approaches developed for MANETs, e. g., topology-based routing protocols, seem unfitting to VANETs; what has been devised for WSNs does often not match the requirements of CPSs; and what has been targeted to CPS applications cannot easily be transferred to WMN application demands. Yet worse: most often, not even the protocol stacks designed to support one class of applications over, e. g., WSNs or VANETs can smoothly be integrated with other applications for the same class of networks.

The reason is that all these networking technologies need to deal with resource scarcity of different kinds and degree (bandwidth, energy, connectivity, etc.). For this reason, for instance, MANET applications in disaster relief need to prioritize critical data traffic due to limited channel capacity, so all nodes in the network need to know about application-specific traffic priorities. WSNs need to aggregate data in order to reduce the packet size, thereby saving energy for communication—a highly application-specific procedure. VANETs require sophisticated, application-tailored dissemination and aggregation strategies to deal with limited bandwidth, changing connectivity, and varying vehicle densities in a highly dynamic topology. More generally speaking, time, energy, bandwidth, connectivity and other constraints prohibit that the network is a pure transport medium: application-level data needs to be understood and processed within the network, not only by "end system" instances of the application logic.

Consequently, application-specific logic is moved into the network: core components of the network need to be tailored to application demands. As a result, a clean separation of "network" and "application" logic in the traditional sense becomes impossible, and protocol layers lose their role as cross-application abstractions. Instead, complex, dedicated protocols are designed for very narrow and specific application scenarios and requirements. The protocols that, e.g., the IETF MANET WG is standardizing are very different from the Geonetworking protocols currently under standardization at ETSI TC ITS. In the end, the impression arises that a whole-system re-design for each application setting and scenario seems inevitable.

However, does this mean that the networks have nothing in common? Such a design perception has severe consequences for the co-existence of applications, for the opportunities to adapt a once-installed network to changing requirements, and for the possibility to integrate new applications into an already deployed system. In car-to-car communication, for instance, it is almost certain that demand for new, additional applications will arise in the future. However, with the current approach to design highly application-tailored protocol stacks, it will be hard to impossible to integrate the corresponding in-network functionality into the then already deployed nodes: the system architecture is constrained to the application and requirements known at the time when it was designed. This unsatisfactory situation may be termed *architectural lock-in*.

If this holds true even within a narrow area like VANET, things are even worse when boundaries between different kinds of ad-hoc networks are crossed. With today's approaches, it is even harder to design systems that provide a basis for, e. g., both a WSN and a WMN.

We therefore pose the question whether it is really necessary (and fruitful) to re-invent the wheel over and over again. Even if protocol layers in the classical sense cannot be carried over from application scenario to application scenario, it still seems likely that a common foundation can be laid. In this paper, we propose the concept of *Context-adaptive Networks* and envision that they could provide such a common basis.

As pointed out, the need to deal with highly varying requirements in different ad-hoc networking scenarios, like resource scarcity, data-dependent networking and processing, or quickly changing network topology and node density, requires that application-specific functionality can be carried out on any node within the system. Context-adaptive Networks aim to provide generic means and abstractions for such a situation-aware and application-aware adaptation of in-network processing.

To this end, applications can deploy functional components on network nodes throughout the network. These functional components are able to perform complex packet and information processing. These components become part of the different networking layers, and they enable to dynamically introduce application-specific behavior into the network stack in an on-demand fashion. Therefore, the core networking framework again becomes application-independent—but in a different sense than pure data-transport networks like the

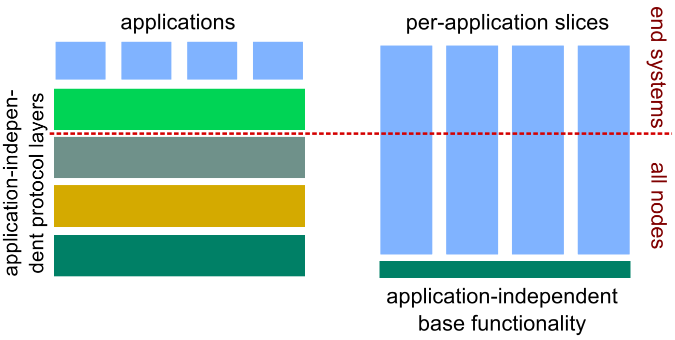

applications
application-independent protocol layers
per-application slices
end systems
all nodes
application-independent base functionality

Figure 1: Layered architecture for data transport-focused networks vs. sliced architecture for application-specific in-network processing.

Internet. Instead of generic protocol *layers* implementing cross-application functionality, such a network comprises application-specific, but vertically isolated *slices*. This is shown in Figure 1.

Slices from different applications can be modified, installed, and removed independently. This allows for a clean abstraction when designing and implementing applications. It also allows to integrate new applications into a running system. In-network processing can be adapted in case the requirements change, without the need of a complete protocol stack re-design for all applications. The networking stack would thus consist of a flexible core framework that is re-configured and extended in an on-demand fashion as new types of application and new forms of communication are introduced.

III. Usage Scenarios

A. Public Safety

Public safety units such as first responders, fire fighters, police, and military need robust communication networks for command and control. On the different hierarchical layers, members of a talk-group communicate via push-to-talk voice channels. Furthermore, the people in charge want to know where their units are. Therefore, command and control systems consist of two main applications: classical push-to-talk voice communication and sensor data transport for self-organizing location maps. The networks must operate reliably even when all infrastructure has been destroyed.

Ad-hoc networks meet the requirements of spontaneous deployment, independence from any kind of existing infrastructure, and robustness in the sense of self-organization and self-healing. However, in larger deployments, quality of service for different applications and priorities of single users are additional requirements. Furthermore, the public safety domain must always be prepared for sudden changes and spontaneous events. Therefore, requirements and priorities may change over the time. Thus, the applications as well as the network have to be able to adapt to the new situation—which, in turn, requires the protocol stack in all nodes to react in highly application-specific ways. This is very hard to implement in a protocol stack where forwarding nodes are application-agnostic. Context-adaptive networking allows to take these application requirements into account in all nodes, without sacrificing a clean system architecture.

B. Urban Sensing

On-going urbanization poses severe challenges to municipalities around the globe. Ever bigger cities need to be managed and maintained and city councils rely on fine-grained sensing data to react on various time-scales to specific developments. One day, it may be important to determine temperature profiles for a certain suburb in order to design buildings for enhanced air flow, the other day one needs to measure fine dust pollution to check whether legal obligations are met. And on another day, an accident at a chemical plant may suddenly give measurement of a specific aerosol highest priority. Ideally, municipalities would deploy generic sensor network nodes with generic chemical sensors throughout the cities that could then be dynamically re-configured to measure specific components with exactly the right application-specific spatial and temporal resolution, with dedicated in-network information processing strategies, and all this while allowing multiple of such measurements to run in parallel.

Context-adaptive Networks will support exactly this kind of scenarios, as it would allow to dynamically adjust a WSN to the specific needs of the measurement task needed by adjusting priorities, in-network processing, and forwarding strategies to match the needs of the sensing applications. In sensor technology research, there are recent trends to investigate and design the flexible sensors that would be needed in addition.

C. Car-to-Car Communication

Car-to-Car Communication and VANETs are currently nearing finalization of standards and are approaching initial deployment. This first generation of systems will include highly specific mechanisms for tasks like geonetworking or distributed congestion control. At the same time, many of these mechanisms implicitly implement design assumptions that may actually not be valid. As an example, geocasting requires specification of a target area and the standards foresee a limited number of ways to specify such an area, e.g., by means of a circular or rectangular shape. If a future application would require a different type of target area, it will not easily be possible to extend the geonetworking implementation in the millions of vehicles that will already be C2C enabled by that time. Updating standards and deployed code-base will be a very cumbersome endeavor. Thus, future applications are limited by the inflexible design of todays standards. Context-adaptive Networks may again offer a solution to this type of problems, as, e. g., determination of target areas and forwarding strategies could be extended when new applications are rolled out.

D. E-Health

In the future, patients and their environment will be equipped with sensors (cf. [7]). Based on heterogeneous sensor data, it will be possible to monitor the health status of a patient. By using actors, it will even be possible to trigger, for instance, the release of a drug to the patient's body. In such a network, the sensor information as well as commands to the actors have to be transmitted in a reliable, robust and fault-tolerant way. Depending on variation of the health status, the requirements to the network will change. New components may be added, with new applications and different requirements to in-network data handling and processing—and the need to integrate smoothly with previously present equipment. A design based on context-adaptive networking ideas would enable all the equipment to participate in the data processing even for applications which have not been present when the network was initially set up, by allowing for new, application-specific functional components be set up in the form of additional slices.

IV. Conclusion and Research Challenges

As seen in the different scenarios, one of the big challenges for different flavors of ad-hoc networks is the need to tailor in-network data processing and communication to the varying requirements of specific applications. These requirements are very diverse: data-consistency, reliability, energy efficiency, privacy, and so forth. The requirements may even change over time, depending on the current situation and environment. We advocate the new concept of Context-adaptive Networking to allow applications to adjust processing and communication at arbitrary points in the network, as required in the specific situation. It therefore allows for the required flexibility that is needed in order to implement demanding applications over resource-constrained networks. At the same time, it provides an abstraction, and therefore facilitates the adaptation to changing requirements, and the integration of new applications in the future.

In order to implement Context-adaptive Networks, a number of key challenges need to be tackled. Mechanisms to deploy functional components (i. e., slices) to network nodes are necessary. These mechanisms must be simple and robust, and it must be possible to employ them in settings where resources are very scarce. At the same time, isolation between slices needs to be considered for functional and security reasons. This includes the question of allocating scarce resources in case of competing slices—fairness and security aspects are immediately evident. On the other hand, it may be desirable to re-use components between slices for efficiency reasons. It also relates to the question how much control a slice needs about the device it is executed on.

Another interesting question is to investigate how much flexibility modern communication hardware will allow. Software-defined radios and cognitive radio approaches may provide the technical basis for extremely flexible Context-adaptive Networks. Finally, it needs to be investigated what basic functionality the core framework needs to provide to allow the desired degree of flexibility in design and implementation of slices.

We feel that it will be worth to tackle these challenges: only then it will be possible to realize flexible designs for ad-hoc networks in the future, which are able to support a broad range of applications, without the need to redesign key elements of the system architecture upon each change in requirements.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123–131, Mar. 2005.

[3] M. Conti, S. Giordano, M. May, and A. Passarella, "From Opportunistic Networks to Opportunistic Computing," *IEEE Communications Magazine*, vol. 48, no. 9, pp. 126–139, Sep. 2010.

[4] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," RFC 2501, IETF Network WG, 1999.

[5] E. Geisberger and M. Broy, Eds., *agendaCPS - Integrierte Forschungsagenda Cyber-Physical Systems*. Springer, 2012.

[6] H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 6, pp. 164 –171, june 2008.

[7] Z. Qin, G. Huang, and Q. Dai, "No room for error: Rfid-enabled smart point-of-care medication process in hospital wards," in *Proc. of the IEEE International Conference on RFID-Technologies and Applications*, 2011, pp. 353–358.

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

95-11 *Thomas Beuter, Peter Dadam*:
Prinzipien der Replikationskontrolle in verteilten Systemen

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

2008-07 *M. Maucher, U. Schöning, H.A. Kestler*
An empirical assessment of local and population based search methods with different degrees of pseudorandomness

2008-08 *Henning Wunderlich*
Covers have structure

2008-09 *Karl-Heinz Niggl, Henning Wunderlich*
Implicit characterization of FPTIME and NC revisited

2008-10 *Henning Wunderlich*
On span-P^{cc} and related classes in structural communication complexity

2008-11 *M. Maucher, U. Schöning, H.A. Kestler*
On the different notions of pseudorandomness

2008-12 *Henning Wunderlich*
On Toda's Theorem in structural communication complexity

2008-13 *Manfred Reichert, Peter Dadam*
Realizing Adaptive Process-aware Information Systems with ADEPT2

2009-01 *Peter Dadam, Manfred Reichert*
The ADEPT Project: A Decade of Research and Development for Robust and Fexible Process Support
Challenges and Achievements

2009-02 *Peter Dadam, Manfred Reichert, Stefanie Rinderle-Ma, Kevin Göser, Ulrich Kreher, Martin Jurisch*
Von ADEPT zur AristaFlow® BPM Suite – Eine Vision wird Realität "Correctness by Construction" und flexible, robuste Ausführung von Unternehmensprozessen

2009-03 *Alena Hallerbach, Thomas Bauer, Manfred Reichert*
Correct Configuration of Process Variants in Provop

2009-04 *Martin Bader*
On Reversal and Transposition Medians

2009-05 *Barbara Weber, Andreas Lanz, Manfred Reichert*
Time Patterns for Process-aware Information Systems: A Pattern-based Analysis

2009-06 *Stefanie Rinderle-Ma, Manfred Reichert*
Adjustment Strategies for Non-Compliant Process Instances

2009-07 *H.A. Kestler, B. Lausen, H. Binder H.-P. Klenk. F. Leisch, M. Schmid*
Statistical Computing 2009 – Abstracts der 41. Arbeitstagung

2009-08 *Ulrich Kreher, Manfred Reichert, Stefanie Rinderle-Ma, Peter Dadam*
Effiziente Repräsentation von Vorlagen- und Instanzdaten in Prozess-Management-Systemen

2009-09 *Dammertz, Holger, Alexander Keller, Hendrik P.A. Lensch*
Progressive Point-Light-Based Global Illumination

2009-10 *Dao Zhou, Christoph Müssel, Ludwig Lausser, Martin Hopfensitz, Michael Kühl, Hans A. Kestler*
Boolean networks for modeling and analysis of gene regulation

2009-11 *J. Hanika, H.P.A. Lensch, A. Keller*
Two-Level Ray Tracing with Recordering for Highly Complex Scenes

2009-12 *Stephan Buchwald, Thomas Bauer, Manfred Reichert*
Durchgängige Modellierung von Geschäftsprozessen durch Einführung eines
Abbildungsmodells: Ansätze, Konzepte, Notationen

2010-01 *Hariolf Betz, Frank Raiser, Thom Frühwirth*
A Complete and Terminating Execution Model for Constraint Handling Rules

2010-02 *Ulrich Kreher, Manfred Reichert*
Speichereffiziente Repräsentation instanzspezifischer
Änderungen in Prozess-Management-Systemen

2010-03 *Patrick Frey*
Case Study: Engine Control Application

2010-04 *Matthias Lohrmann und Manfred Reichert*
Basic Considerations on Business Process Quality

2010-05 *HA Kestler, H Binder, B Lausen, H-P Klenk, M Schmid, F Leisch (eds):*
Statistical Computing 2010 - Abstracts der 42. Arbeitstagung

2010-06 *Vera Künzle, Barbara Weber, Manfred Reichert*
Object-aware Business Processes: Properties, Requirements, Existing Approaches

2011-01 *Stephan Buchwald, Thomas Bauer, Manfred Reichert*
Flexibilisierung Service-orientierter Architekturen

2011-02 *Johannes Hanika, Holger Dammertz, Hendrik Lensch*
Edge-Optimized À-Trous Wavelets for Local Contrast Enhancement with Robust Denoising

2011-03 *Stefanie Kaiser, Manfred Reichert*
Datenflussvarianten in Prozessmodellen: Szenarien, Herausforderungen, Ansätze

2011-04 *Hans A. Kestler, Harald Binder, Matthias Schmid, Friedrich Leisch, Johann M. Kraus (eds):*
Statistical Computing 2011 - Abstracts der 43. Arbeitstagung

2011-05 *Vera Künzle, Manfred Reichert*
PHILharmonicFlows: Research and Design Methodology

2011-06 *David Knuplesch, Manfred Reichert*
Ensuring Business Process Compliance Along the Process Life Cycle

2011-07 *Marcel Dausend*
Towards a UML Profile on Formal Semantics for Modeling Multimodal Interactive Systems

2011-08 *Dominik Gessenharter*
Model-Driven Software Development with ACTIVECHARTS - A Case Study

2012-01 *Andreas Steigmiller, Thorsten Liebig, Birte Glimm*
Extended Caching, Backjumping and Merging for Expressive Description Logics

2012-02 *Hans A. Kestler, Harald Binder, Matthias Schmid, Johann M. Kraus (eds):*
Statistical Computing 2012 - Abstracts der 44. Arbeitstagung

2012-03 *Felix Schüssel, Frank Honold, Michael Weber*
Influencing Factors on Multimodal Interaction at Selection Tasks

2012-04 *Jens Kolb, Paul Hübner, Manfred Reichert*
Model-Driven User Interface Generation and Adaption in Process-Aware Information Systems

2012-05 *Matthias Lohrmann, Manfred Reichert*
Formalizing Concepts for Efficacy-aware Business Process Modeling*

2012-06 *David Knuplesch, Rüdiger Pryss, Manfred Reichert*
A Formal Framework for Data-Aware Process Interaction Models

2013-01 *Matthias Frank, Frank Kargl, Burkhard Stiller*
Abstract Proceedings of the 7th Workshop on Wireless and Mobile Ad-Hoc Networks (WMAN 2013)

2013-02 *Andreas Lanz, Manfred Reichert, Barbara Weber*
A Formal Semantics of Time Patterns for Process-aware Information Systems

2013-03 *Matthias Lohrmann, Manfred Reichert*
Demonstrating the Effectiveness of Process Improvement Patterns with Mining Results*

2013-04 *Semra Catalkaya, David Knuplesch, Manfred Reichert*
Bringing More Semantics to XOR-Split Gateways in Business Process Models Based on Decision Rules

2013-05 *David Knuplesch, Manfred Reichert, Linh Thao Ly, Akhil Kumar,*
Stefanie Rinderle-Ma
On the Formal Semantics of the Extended Compliance Rule Graph

Ulmer Informatik-Berichte
ISSN 0939-5091

Herausgeber:
Universität Ulm
Fakultät für Ingenieurwissenschaften und Informatik
89069 Ulm