[KAHSt06] *Andre König, Ralf Ackermann, Matthias Hollick, Ralf Steinmetz;* **Geographically Secure Routing for Mobile Ad Hoc Networks: A Cross-Layer Based Approach;** International Conference on Emerging Trends in Information and Communication Security (ETRICS 2006), Freiburg, June 2006, S.

Geographically Secure Routing for Mobile Ad Hoc Networks: A Cross-Layer Based Approach

André König, Ralf Ackermann, Matthias Hollick, and Ralf Steinmetz

Multimedia Communications Lab (KOM)
TU Darmstadt
Merckstrasse 25
64283 Darmstadt
{Andre.Koenig, Ralf.Ackermann, Matthias.Hollick,
Ralf.Steinmetz}@KOM.tu-darmstadt.de

Abstract. The growth of mobile and wireless communications has also raised various concerns with respect to information-security. Recently, the design of secure protocols for wireless LANs has been placed under scrutiny to ensure the authenticity, integrity, and confidentiality of the communication. However, these protocols mostly focus on the protection of the ongoing communication only and neglect long-term security goals. Attack vectors against such long-term security goals include, but are not limited to adversaries that are eavesdropping the wireless communication to perform a post hoc cryptanalysis (possibly years after the data-capture). This paper introduces the paradigm of geographically secure routing to address the aforementioned shortcomings of existing security schemes. In particular, we propose a solution to transmit sensitive information in a mobile ad hoc network such that the routes are restricted to trustworthy nodes. Our scheme is able to prevent eavesdropping of or tampering with data in-flight, thus, thwarting passive and active attacks and supporting the long-term security of the system. We implement our solution using a cross-layer approach that builds on existing ad hoc routing protocols and maintains the compatibility with these protocols. A simulation study shows the feasibility of our approach and validates the proposed solution.

1 Introduction

1.1 Motivation

The growth of mobile and wireless communications has also raised various concerns with respect to information-security. Several breaches in security protocols for wireless communication systems based on IEEE 802.11 Wireless LAN, Bluetooth, or GSM have recently been reported. As a result, the design of secure protocols in the wireless communication domain has been placed under scrutiny to ensure the authenticity, integrity, and confidentiality of the communication.

Mechanisms and protocols such as WEP, WPA, IEEE802.11i on lower layers are combined with higher layer mechanisms such as IPSec and TLS to meet the security demands. Since these approaches are all based on currently available encryption mechanisms, they are potentially vulnerable regarding their long-term security. Attack vectors against such long-term security goals include, but are not limited to adversaries that are eavesdropping the wireless communication to perform a post hoc cryptanalysis. The mathematical problems that build the fundament of todays encryption algorithms might be solved in affordable time in the future if we consider improvements in computing power, e.g., based on advances in quantum computing [1]. The breaking of the DES algorithm, as described in [8], is one example of the past that surely will show up again. In summary, the application of traditional security schemes in wireless networks opens up various problems that demand for novel solutions. This paper introduces the paradigm of geographically secure routing to address the aforementioned shortcomings of existing security schemes. In particular, we propose a solution to transmit sensitive information in a mobile ad hoc network such that the routes are restricted to trustworthy nodes. Our scheme is able to prevent eavesdropping of or tampering with data in-flight, thus, thwarting passive and active attacks and enhancing the long-term security of the system.

1.2 Contribution

In this work we investigate novel mechanisms to support the long-term security coupled to mobile/wireless ad hoc networks. We develop a solution to provide geographically secure routes on top of legacy routing protocols such as Dynamic Source Routing (DSR). Our solution follows a cross-layer approach to control the routing protocol from application level. Our main contribution is the design, implementation, and experimental validation of a geographically secure routing scheme. We follow a cross-layer approach to couple the application layer (which specifies the security requirements) with the network layer (here: legacy ad hoc routing protocols). Our solution aims to enhance the long-term security of corporate ad hoc network deployments.

1.3 Outline

The remainder of this paper is structured as follows. In Section 2, we describe the scenario underlying our work. We perform a security analysis and derive the requirements for possible solutions. Our novel approach towards geographically secure ad hoc routing is precisely described in Section 3. In particular, we motivate the choice of a cross-layer architecture for our solution and give a description of the routing control interface that includes all necessary protocol extensions. As a proof-of-concept we perform a simulation study to validate the operation of our routing mechanism. We outline the design of the simulations and analyze and present selected results in Section 4. Finally, we summarize our work in Section 5.

2 Scenario

Within our scenario we consider a research site with employees and visitors carrying mobile communication devices. Visitors have to be considered as non-trustworthy and are therefore assumed to be restricted to a designated area within the research site. Employees are considered as trustworthy. For them, no restrictions with respect to movement are made.

From the technical point of view, trusted employee devices are further divided into devices whose functionality can be changed with small effort (like notebooks or PDAs running open source operating systems) and devices where this is not (easily) possible (like network printers with proprietary operating systems).

Our approach is based on an extension of the functionality of nodes. Nodes, whose functionality we extend, are further called *extended nodes*. Nodes with unchanged functionality are referred to as *standard nodes*.

For communication between any two involved devices, we use a mobile ad hoc network. The exchanged information is classified into confidential and non-confidential data flows. To setup the required routes, the deployed routing protocol is DSR [5].

From the described scenario, we can extract four possible communication cases, which are shown in Figure 1:

- Employee nodes exchanging confidential information
- Employee nodes exchanging non-confidential information
- Employee node and visitor node exchanging non-confidential information
- Visitor nodes exchanging non-confidential information

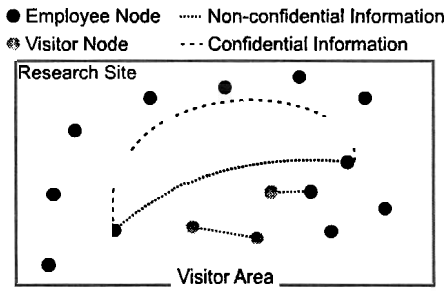


Fig. 1. Scenario with schematic end-to-end communication relationships

2.1 Security Analysis

Various attacks that are inherently possible in mobile ad hoc networks due to their infrastructureless nature have been identified so far [6]. These can be classified into active and passive attacks. In general, the intention of an active attack

is to change the data flow in a mobile ad hoc network. For this, active attacks require changes in the behavior of the deployed routing protocols to achieve the desired effects. Thus, nodes that perform active attacks, can be detected (and located) by an intrusion detection system, as proposed for example in [7]. In contrast to this, passive attacks like traffic analysis or eavesdropping of specific communications do not require the attacker to change the routing protocol and have no direct effect on the behavior of the mobile ad hoc network as a whole. In fact, passive attacks do not require the node to transmit any information, what makes it (nearly) impossible to detect passive attackers. Active attack mechanisms may (but do not have to) be used in combination with eavesdropping in order to make the result even worse (or better from the perspective of the attacker).

Today, data encryption is the method of choice, to prevent that information collected during an eavesdropping attack can be exploited by the attacker. In view of long-term security, state of the art encryption mechanisms could fail in a few years, giving the potentially malicious visitor in our scenario the chance to reveal the secrets once collected. If we further consider public key infrastructures [2], where a private/public key pair is usually used for a long period of time, it might be possible for an adversary to compute the private key from collected data and to later still misuse this knowledge. From this perspective, a feasible way to keep information confidential in the future with today's techniques is to keep it away from unauthorized persons.

For our given scenario, we expect all attacks, whether they are of active or passive nature, to be restricted to the visitor area. The consequence is that confidential information should not enter the visitor area. This is shown in Figure 1 where end-to-end communication relationships are sketched.

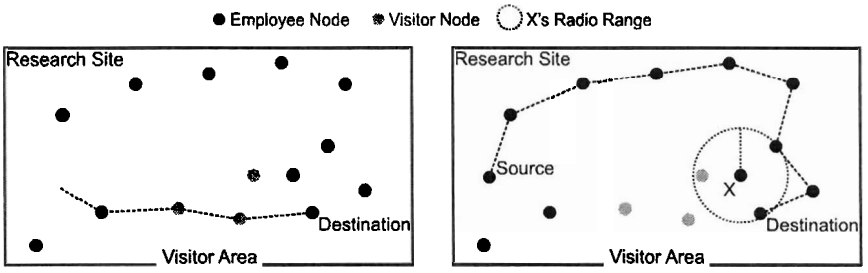
2.2 Resulting Requirements

In the cases of non-confidential communication, the visitor nodes should be used for hop by hop information forwarding in order to provide the expected connectivity. A respective route in our scenario is shown in Figure 2(a). This route will most likely be chosen by DSR since it is the shortest with respect to number of hops.

In the case of a confidential communication between employee nodes, a visitor node should (for the reasons described in the previous section) not be part of a path between employee nodes. So at the first stage, we need the ability of an explicit user interaction or an implicit policy mechanism within the utilized application to inform the routing process whether or not the information to transmit is confidential.

For confidential communications, we have to establish routes which bypass the visitor area. Figure 2(b) shows a route in our scenario that meets this restriction.

When we take a look at node X in Figure 2(b), we see that due to its proximity to the visitor area, its transmission would also reach unauthorized



(a) Non-confidential route (b) Confidential route

Fig. 2. Confidential versus non-confidential route

nodes. Even though X is a trusted employee node, it should at its current position not be used for forwarding confidential information.

For the decision whether an employee node may be contained in a route that is used for confidential communication, information about its position and its radio range has to be available.

With respect to the subclassifications of employee devices, we have to assume that connectivity decreases if we restrict routes to employee nodes whose routing functionality we extended to distinguish between confidential and non-confidential communication and to handle position information (extended nodes). To overcome this, we allow a route to contain a certain number of non-extended employee nodes (standard nodes) between any two adjacent extended nodes. The endpoints of a route, that is sender and receiver, are expected to be extended nodes.

The properties of our scenario and the requirements can be summarized as follows:

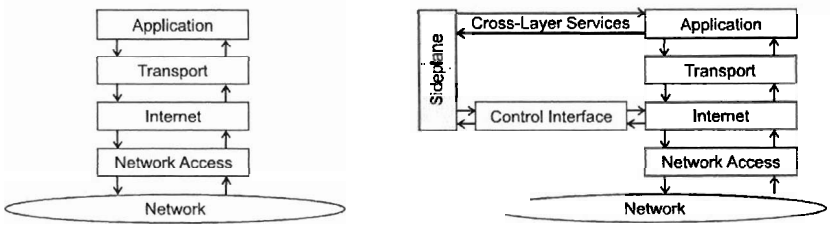
- Devices are classified into employee devices and visitor devices
- Visitor devices are restricted to the visitor area
- Employee devices are further classified into extended nodes and standard nodes
- End points of communications are extended nodes
- An information exchange between application and routing process is needed
- Knowledge of the position and the radio range of extended nodes has to be available

3 Approach

To achieve the desired functionality as described in the previous section, we have to take influence on the vertical control flow within one node (from application to routing process) as well as on the horizontal data flow between two nodes. In the following, we describe the required extensions.

3.1 Cross-Layer Architecture

For reasons of compatibility, we base our approach on the well established Internet model with its strictly separated layer architecture, as shown in Figure 3(a). To exchange the necessary information between the application and the routing process, we add a cross-layer extension similar to the design proposed in [3] in a two step process.



(a) Internet layer model (b) Cross-layer design

Fig. 3. Extension of the Internet layer model

In the first step an additional control interface which will be described in detail in the next section is attached to the network layer. This way, the desired influence on the routing process becomes possible. A similar approach with the aim to rewrite routing tables in order to optimize Gnutella networks is presented in [4].

Step two adds an orthogonal sideplane, which offers the service primitives for cross-layer communication. A draft of the resulting architecture is given in Figure 3(b).

The sideplane is organized as a lightweight data structure containing *(name, value)* tuples. Services are offered to add and change tuples, as well as to register a process to be informed about changes in a specific tuple. With respect to our scenario, an application adds and changes tuples as for example the required position information of the node *("NodePosition", GPS coordinates)* and the visitor area *("VisitorArea", Polygon)*. The control interface of the network layer registers for changes in both tuples. The information is then used to influence the routing process respectively.

3.2 Routing Control Interface

To stay compatible with nodes that run a standard DSR protocol, we leave the DSR header unchanged. The necessary information is contained in an additional header that follows the DSR header. We assign the header number *253* that is reserved by IANA for experimentation and testing. Thus the value of the *next header* field of the DSR header (which itself has not been assigned a fixed

number yet) is *253* and points to our additional header. The resulting MAC frame is shown in Figure 4.

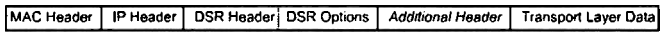


Fig. 4. MAC frame with additional header

Nodes that run a standard DSR protocol simply ignore the additional header, whereas nodes that are equipped with our extension can read and evaluate the contained information. We define three header formats for the three phases of a communication which are route request, route reply and data transfer:

Route Request To provide security at the earliest possible point in time, we already demand the route request not to reach the visitor area. This way, we prevent visitors to perform traffic analysis or (if able to handle our extension) to pretend a position outside the visitor area with the aim to be included in a confidential route.

For the route discovery phase, the additional header contains the following information:

Next Header This is used to determine the transport layer protocol as for example TCP or UDP.

TTL The time to live for this route request. This field is decreased at each extended node by the number of hops that where traversed since the previous extended node. If we allow a route to only consist of extended nodes, TTL will be decreased by one at each (extended) node. If standard nodes are allowed to be situated between extended nodes, TTL is decreased respectively.

Max. intermediate standard nodes This field specifies the maximum amount of standard nodes that may be situated between two adjacent extended nodes. The TTL of the IP header is set to this value at every extended node. This way, the broadcast of a route request that will be done by standard DSR nodes is restricted to the desired amount of standard nodes between adjacent extended nodes.

Expected Replies The amount of expected route replies which will be of relevance for our multipath approach as a part of our future research.

Sequence Number This field is reserved for our multipath approach.

Header Length The overall length of the additional header. The length is not fixed, since the following field contains a flexible description of the position and the shape of the visitor area.

Restricted Area A polygonal model of the visitor area.

Figure 5 depicts the resulting structure of the additional header for the route request phase.

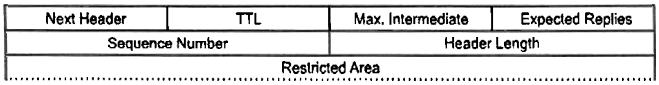


Fig. 5. Header format for route request

Route Reply During the route reply phase, each extended node appends its current geographical position and its position in the recorded list of hops in the DSR options to the extended header. The resulting header format is shown in Figure 6.

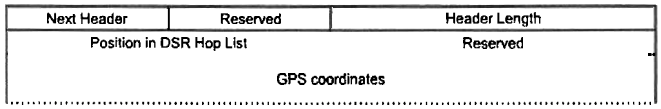
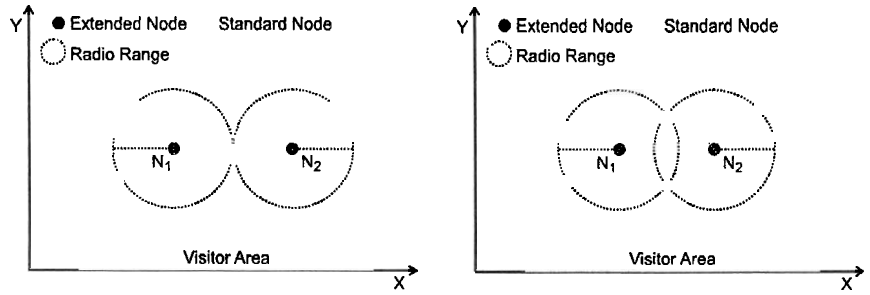


Fig. 6. Header format for route reply

Based on this information, the source evaluates the degree of security, a route can offer. As an example, we assume that one standard node is situated between two extended nodes. For a worst case scenario, we further assume each extended node to be as close to the visitor area as it is allowed by its radio range.

If the distance between the extended nodes then converges to the sum of their radio ranges, the transmission of the intermediate standard node can not reach the visitor area, as shown in Figure 7(a).



(a) Secure route (b) (Possibly) unsecure route

Fig. 7. Route with one intermediate standard node

If, on the other hand, the distance between the extended nodes is smaller than the sum of their radio ranges, the transmission of the intermediate standard node may well reach the visitor area. Regarding this, a quantitative assertion about

the security of a route becomes possible. The possibility that the transmission of an intermediate node reaches the visitor area can be calculated from the knowledge of the position of the two neighboring extended nodes. Figure 7(b) depicts the worst case of a (possibly) unsecure situation. We have to notice, that the intermediate standard node could be situated anywhere within the intersecting plane of the radio ranges of the extended nodes.

Data Transfer During the phases of route request and route reply, we established a route, that meets our security requirements. Since we are confronted with mobile devices, the route has to be maintained with respect to security during the data transfer phase.

To obtain the required flexibility for our further work on more unrestricted scenarios, we define a header for the data transfer phase, that may be used optionally when the scenario (and thus the restrictions with respect to security) changes. The header therefore contains for each extended node in the DSR hop list a description of an area, where the node is allowed to detain. If a node leaves this area, it has to stop forwarding messages for the respective communication.

Figure 8 shows the additional header that is used during the data transfer phase.

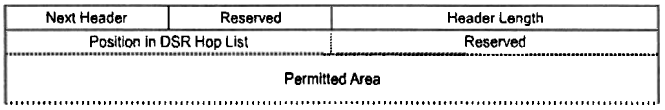


Fig. 8. Header format for data transfer

4 Simulation and Evaluation

We apply the methodology proposed by Jain [9] for the experimental analysis of our approach and adopt the individual steps to our scenario. The methodological steps can be summarized as follows:

- Definition of the system, goals, and services
- Selection of the metrics
- Definition of the parameters to study
- Selection of the factors/elements of the parameter set
- Choice of the evaluation technique
- Selection of the workload
- Design of the individual experiments
- Analysis and interpretation of the obtained data
- Presentation of the results

4.1 Simulation Setup

A detailed description of the simulation setup regarding the dimensions is shown in Figure 9. We consider a research site of 3000 meters width and 2000 meters height. The visitor area is situated at the center of the bottom line with a width of 1000 meters and a height of 500 meters. The radio range of 250 meters is equal for each node within our scenario. No packets are lost during transmission.

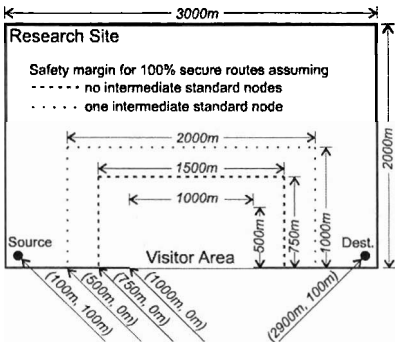


Fig. 9. Dimensions of our scenario

To obtain a worst-case scenario for our approach, we place the source and the destination in the lower left and the lower right corner of the research site. If successful, our approach discovers a route which bypasses the visitor area, whereas we expect standard DSR to discover a route straight through the visitor area, as we already drafted in Figure 2.

The utilized simulation tool is an adapted version of JiST/SWANS [10], a Java based open source discrete event simulator for wireless ad hoc networks. JiST/SWANS has shown to be easy extendable and to provide good scalability and performance.

In a first step, we compare the connectivity of standard DSR to the connectivity of our approach. As a metric for this we use the fraction of successful route requests out of the number of total route requests. A statistical mean value is determined during 1000 simulation runs with random node placement and one route request each. Sender and receiver are placed at the fixed positions as shown above. Each extended node with a position outside the inner safety margin shown in Figure 9 (so at least the sending range of 250 meters away from the visitor area) is allowed to be contained in a route.

For this evaluation, the parameters for each 1000 runs are

- the total number of nodes in the scenario,
- the fraction of extended nodes, and
- the number of intermediate standard nodes between two adjacent extended nodes.

In the second step, we quantitatively evaluate the degree of security that is reached, if we allow one intermediate standard node to be situated between two adjacent extended nodes. For this, we choose a fixed parameter set, that showed to achieve 100% connectivity in the first step of evaluation described above. We then introduce a second safety margin, as shown in Figure 9. No extended node that is situated within this area is allowed to forward messages. It is obvious that if this second safety margin then has the size of 250 meters (measured from the inner margin), no messages reach the visitor area, since the sending range of an extended node and a following standard node can at most be 500 meters.

For the second step, the parameter that is considered in simulation is the width of the outer safety margin. Again, we perform 1000 simulation runs with random node placement and one route request each. Sender and receiver stay fixed at the positions shown in Figure 9. To check whether a discovered route is in reception range of the visitor area, we modeled listening nodes for JiST/SWANS. These are placed with a distance of 100 meters along the boundaries of the visitor area. The listening nodes do not forward any messages and thus have no effect on the route discovery process. The metric to measure the security of a route is the fraction of route request messages that are received by the listening nodes around the visitor area out of the total amount of route request messages that are sent during the route request phase.

4.2 Simulation Results and Evaluation

To graphically show that our approach works in general, Figures 10 and 11 provide screenshots of the route request phases of our approach and DSR. The visualization is done with a graphical monitoring tool for the JiST/SWANS simulator which has been developed at our institute. We model a static simulation setup, that is similar to the scenario as depicted in Figure 2.

In Figures 12 and 13, the results of the first step of the evaluation of our approach are shown. Figure 12 depicts the evaluation of the connectivity of our approach and of DSR. For this evaluation we used homogeneous setups, which consist either of standard DSR nodes or of extended nodes.

As we expected, the price for a secure route is a decrease in connectivity of our approach compared to standard DSR. The mean decrease in connectivity for our scenario shows to be approximately 20%. The elaboration of the reason for this will be part of our future work.

For the evaluation shown in Figure 13, a heterogeneous setup of standard and extended nodes is considered. Depicted is the connectivity of routes which only consist of extended nodes and of routes which may contain one intermediate standard node between adjacent extended nodes. We simulate a random distribution of 400 nodes and stepwise increase the fraction of extended nodes.

In Figure 14 the results of the second step of our evaluation are presented. We simulate a setup with 200 standard nodes and 200 extended nodes. One intermediate standard node is allowed to be situated between two adjacent extended nodes. The size of the outer safety margin is increased stepwise.

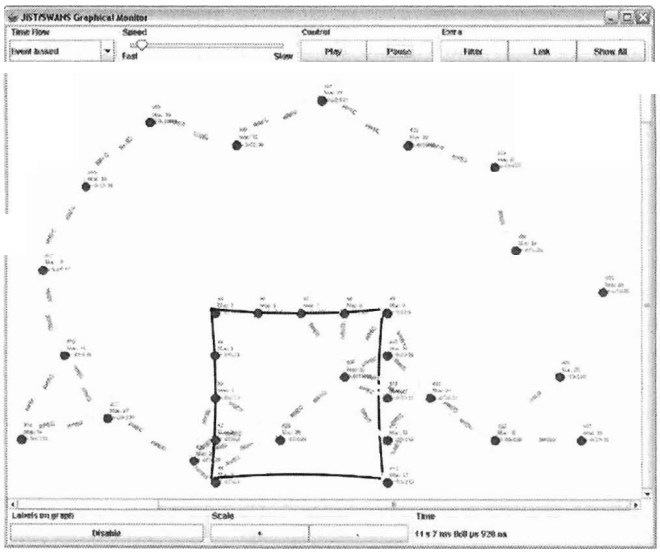


Fig. 10. Standard DSR route request

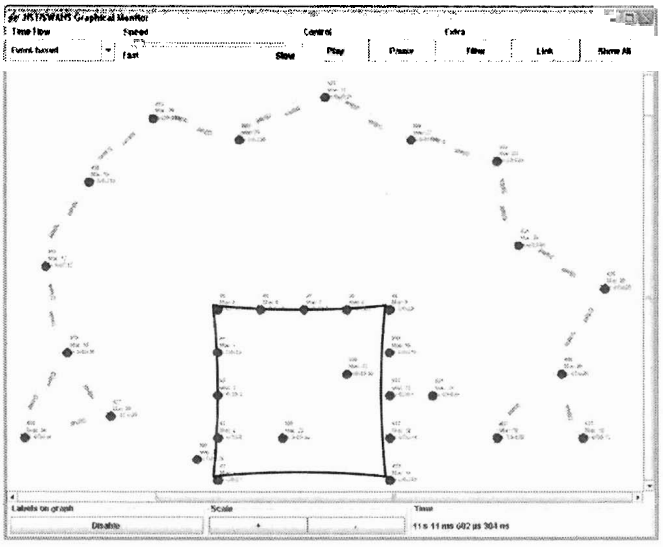


Fig. 11. Restricted route request

Like presumed, the degree of security of a route decreases if we allow standard nodes to be contained in a route and along with this reduce the size of the outer safety margin. The explanation for this observation is that like DSR, our

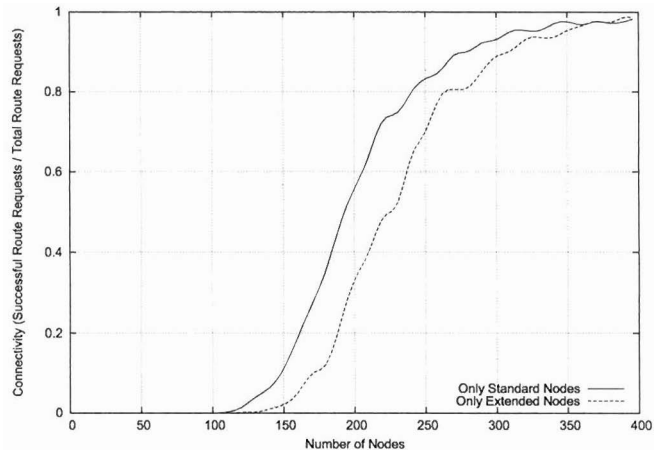


Fig. 12. Connectivity of DSR and our approach

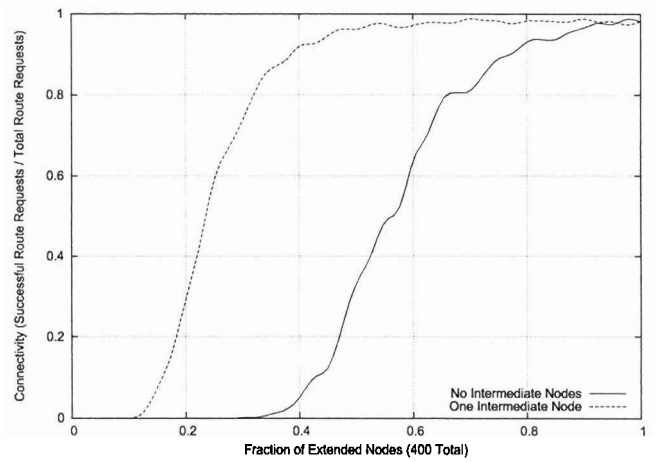


Fig. 13. Connectivity for routes with none and one intermediate standard node

approach will most likely find the shortest route with respect to number of hops. This route is most likely the one with the shortest distance to the visitor area. Therefore, as shown in Figure 7, the transmission of an intermediate standard node can reach the visitor area, if the distance between the neighboring extended nodes is smaller than the sum of their radio ranges. In this evaluation, our approach always performs better than standard DSR. For our scenario, DSR shows to have a constant rate of 50% intercepted route request messages out of the total amount of transmitted route request messages.

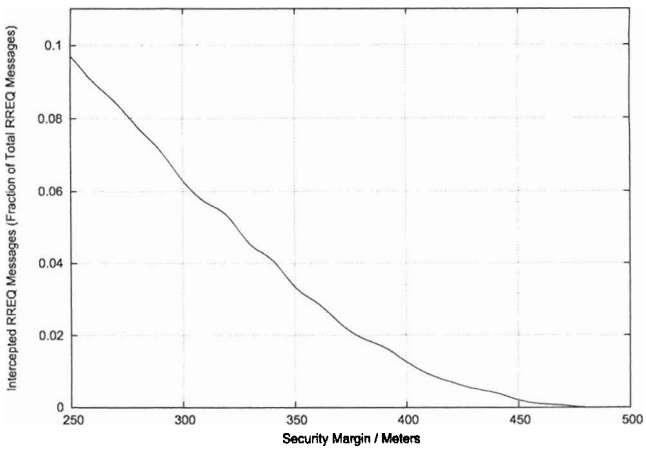


Fig. 14. Quantitative security of our approach

Summary and Outlook

Keeping away confidential information from unauthorized persons turns out to be a feasible support for today's available security mechanisms. This especially holds for scenarios with a demand for long-term security.

Through a cross-layer extension of the existing Internet layer model, we achieve interaction between the different layers. This enables us to restrict routes in mobile ad hoc networks to nodes which meet our security requirements and therefore to prevent that their transmission reaches non-trustworthy nodes.

Routing with regard to the geographical position of nodes with extended functionality and number of intermediate nodes with unchanged functionality as two degrees of freedom have been our concerns for now. Our scenario quickly reaches a high complexity when we take more than two (visitor, employee) levels of trustworthiness into account. Also a dynamic change of these levels may be necessary, when an employee enters the visitor area. Furthermore, visitors may be allowed to move relatively unrestricted throughout the research site. These more realistic and thus more complex scenarios will be the focus of our future research.

Within these scenarios, also temporal aspects will be part of our research. As an example we plan to delay sending on transport layer in order to prevent a high security level node from transmitting while in proximity to a low security level node. We furthermore will consider the adaptation of the transmission power of nodes to increase the number of possible routing devices and with this further improve connectivity.

References

1. G. Brassard; Cryptology Column - Quantum Computing: The End of Classical Cryptography?; Département d'informatique et de R.O. Université de Montréal; ACM Digital Library; 1994
2. David Henry; Who's Got the Key?; University of Maryland; SIGUCCS 1999
3. M. Conti, J. Crowcroft, G. Maselli, G. Turi; A modular cross-layer architecture for ad hoc networks; In Jie Wu, editor, Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks; CRC Press LLC, 2004
4. M. Conti, E. Gregori, G. Turi; A Cross-Layer Optimization of Gnutella for Mobile Ad hoc Networks; Istituto di Informatica e Telematica - CNR; Pisa, Italy; ACM Digital Library; Presented on MobiHoc 2005
5. D.B. Johnson, Rice University, D.A. Maltz, Carnegie Mellon University, Y. Hu, Rice University; The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR); IETF MANET Working Group, Internet-Draft, 2004
6. **B. Wu,** J. Chen, J. Wu, and M. Cardei; A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks; accepted to appear in Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D. -Z. Du (eds.), Springer, 2006
7. Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, Karl Levitt; Intrusion detection: A specification-based intrusion detection system for AODV; Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks; October 2003
8. Electronic Frontier Foundation; Cracking DES - Secrets of Encryption Research, Wiretap Politics & Chip Design; O'Reilly, 1998
9. Raj Jain; The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling; Wiley-Interscience, 1991
10. Rimon Barr; JiST - An efficient, unifying approach to simulation using virtual machines; PhD dissertation; Cornell University; May 2004