KHL S09

[KHLS09] *André König, Matthias Hollick, Christoph Linck, Ralf Steinmetz;* **On the Implications of Adaptive Transmission Power for Assisting MANET Security.** In: Christian Poellabauer, Liqiang Zhang, Habib M. Ammari: In Proceedings of the Third IEEE International Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN 2009), June 2009. Seite

On the Implications of Adaptive Transmission Power for Assisting MANET Security

André König, Matthias Hollick, Ralf Steinmetz
Multimedia Communications Lab (KOM)
Technische Universität Darmstadt
Darmstadt, Germany
{andre.koenig, matthias.hollick, ralf.steinmetz}@kom.tu-darmstadt.de

Abstract

Mitigating misbehavior in mobile ad hoc networks (MANET) requires effective intrusion response systems. In this work, we present an intrusion response scheme that is tailored to support the infrastructureless nature of MANETs. We propose a geographic solution towards excluding misbehaving nodes which is robust against address spoofing from the attacker. In particular, we investigate how an adaptive transmission power can be used to physically keep communication away from misbehaving nodes. We present different strategies for adapting transmission power taking into account effects of asymmetric links, and we provide a detailed performance evaluation based on a series of simulation studies. Our results show that the proposed solution significantly reduces the artificial packet loss that is introduced by geographic intrusion response strategies. Yet, we further observe side-effects of an adaptive transmission power on standard (non power-aware) MANET routing protocols.

1. Introduction

Due to the wirelessly connected devices and the infrastructureless nature, MANETs lack well defined network borders. Further, MANETs compensate the absence of a communication infrastructure by building upon the cooperation of the devices involved. As a consequence, MANETs are beyond the protection of traditional security mechanisms. In addition to current attack vectors, new ways of potential misbehavior have been identified from physical to application layer in e.g. [1] and [2]. At the same time, MANETs are envisioned for deployment in sensitive scenarios like emergency response operations where the constant availability of communication services is an essential security objective. Thus, effective security mechanisms are needed for MANETs to become ready for real-world deployment.

Secure routing protocols such as SAODV [3] and Ariadne [4] have been proposed as preventive security measures for MANETs. Though thoroughly designed, these protocols have been shown to be susceptible to attacks, recently in [5]–[7]. Further, secure routing protocols are in general not able to prevent attacks on other layers than the network layer.

Intrusion detection systems (IDS) in combination with intrusion response systems (IRS) are a promising approach to recover network operation in case of subverted preventive security measures. Although IDSs for MANETs have been studied comprehensively, only minor attention has been paid to appropriately reacting to intrusions detected. Mostly, as in [8]–[10], address-based solutions have been proposed. In [11] we have shown that this should not be the sole method of choice for MANETs where devices are from many administrative domains (possibly one per device) and, thus, changing addresses is possible with little effort. Instead of taking IRS actions based on addresses, we have proposed to exclude misbehaving devices from the network based on their geographical position. For this, we establish quarantine zones around positions where misbehavior has been detected. Communication is not allowed to enter or leave these quarantine zones. This way, we create (temporary) network borders separating the operational areas of the network from areas affected by misbehavior.

Although this location-based IRS has shown to be immune against misbehaving nodes changing addresses, it is limited by inherent drawbacks. In its naïve version, quarantine zones are of the size of the transmission range of nodes. As a first drawback, this results in quite a large number of benign nodes that are located in quarantine zones and, thus, are excluded from the network. Second, routes between benign nodes outside quarantine zones are interrupted due to intermediate nodes being located in quarantine zones. We consider these drawbacks, as shown schematically in Figure 1, to be the most severe ones. Intuitively, if we manage to minimize the size of quarantine zones, we will reduce these unwanted effects of the location-based IRS.

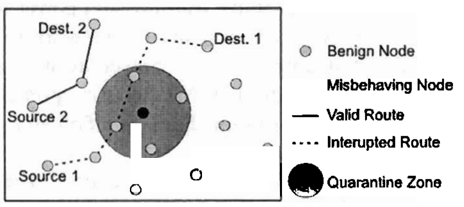


Figure 1. Drawbacks of the location-based IRS

In this paper, we show how an adaptive transmission power of devices can be used to reduce the size of quarantine zones. After presenting related work, we provide a brief description of *GeoSec*, our location-based IRS. We introduce how *GeoSec* can be extended by an adaptive transmission power and propose different approaches for this. The focus of our evaluation lies on the resulting (positive and negative) effects of adaptive transmission power with respect to the size of quarantine zones and node mobility.

2. Related Work

Related work that has motivated and influenced our research can be found among geographical approaches in MANETs and among application domains for adaptive transmission power.

2.1. Geographical Approaches in MANETs

Several routing mechanisms for MANETs that take into account geographical information of nodes have been proposed. An overview can be found e.g. in [12]. Two of these protocols which are related to our work are LAR [13] and DREAM [14]. Both protocols use location information to restrict the propagation of broadcast messages as it is done in *GeoSec*.

A precondition for LAR and DREAM as well as for our approach is that nodes are aware of their geographical position. One way to determine this would be the use of GPS [15]. Besides that, other approaches for the determination of positions in dynamic environments have been proposed. A survey can be found in [16]. The localization mechanisms presented there were developed for sensor networks but can also be applied to mobile ad hoc networks. The approaches can be categorized according to whether the outcome is a globally unique position or a position relative to a specific, local neighbourhood. Since our approach neither requires globally available information nor globally unique positioning, most of the localization approaches proposed can be used in combination with *GeoSec*.

2.2. Adaptive Transmission Power

Adaptive transmission power has a wide range of applications in wireless networks. Saving battery power or signal strength control for CDMA based systems are prominent examples. In MANETs, adaptive transmission power is mainly used for controlling and optimizing the network topology.

One of the first approaches of power aware routing in MANETs is proposed in [17]. Metrics for optimal routing with respect to energy consumed are specified and validated by simulation.

Distributed heuristics for topology control without the necessity to exchange additional control information are proposed in [18].

A distributed protocol for topology control in order to achieve a connected network by adapting transmission power such that an optimal number of neighbours per node is maintained, is proposed in [19]. In contrast to [18], control messages are needed.

Algorithms for adaptive network-global as well as individual transmission power in MANETs with the goal to achieve a maximized throughput (not minimal energy) subject to the network load and the network density (nodes per area) have been proposed in [20]. No additional messages are needed, but for individual transmission power the 802.11 protocol is extended to prevent asymmetry.

A protocol for maximizing network lifetime by adaptive transmission power on a per-node basis has been proposed in [21]. The algorithm works in a distributed way and, for this, requires the exchange of corresponding protocol messages.

To the best of our knowledge, no related work exists that utilizes an adaptive transmission power in the context of location-based security mechanisms for MANETs.

3. Architecture

We now describe the components upon which we build in order to perform location-based intrusion response. We provide a summary of the first version of *GeoSec* based on which we propose add-ons for adaptive transmission power. We further provide a brief description of the IDS and the location service as well as of the attack mechanism considered.

3.1. The Black Hole Attack

To obtain a worst-case misbehavior, we focus on an aggressive version of the black hole attack that has a devastating effect on network performance. A black hole attracts any communication which is, subsequently, dropped instead of being forwarded to the actual receiver. This is achieved by pretending attractive routes regarding the metrics of the routing protocol deployed. We implemented the black hole behavior for the routing protocol AODV which we utilize in our studies. In this case, attractiveness of routes is defined by their length (in hops) and their age. Therefore, the black hole claims that the destination intended is its direct neighbor. Additionally, the routes offered by the black hole appear to be newer than routes offered by the destination. This way, the route offered by the black hole will be preferred by AODV.

3.2. The Location Service

To simplify the implementation, our location service is based on the bird's eye view that is available in our simulation tool. To increase realism, we introduce a positioning delay t_{pos}. As mentioned, the globally available position information that is provided by our location service is not a necessary precondition for *GeoSec*. Since quarantine zones are managed on a per-node basis, operation is possible based on location information that is available locally (in the neighborhood of a malicious node) only.

3.3. The IDS

Since it is not our goal to develop a new IDS approach for MANETs, our IDS is trimmed to provide a reasonable detection performance of our implementation of the black hole attack. We adjusted the parameters such that the IDS achieves a performance that is comparable to that of other systems proposed in literature. Similar to OCEAN [10], our IDS works based on local information only. Attack detection is performed in two steps. During a monitoring interval t_{mon}, a node X keeps track of the forwarding behavior of its neighbors (we call node Y a neighbor of node X if it is within X's transmission range). For each of its neighbors, X maintains a counter n_{rec} for packets that Y has received for forwarding. A second counter n_{forw} is maintained for packets that Y forwarded correctly. After each monitoring interval, X calculates a rating r_Y that describes the forwarding behavior for Y. We use a weighting factor $w_{balance} \geq 1$ to balance the counters n_{rec} and n_{forw}. With this, r_Y is calculated as

$$r_Y = \frac{n_{rec}}{w_{balance}} - n_{forw}$$

If r_Y exceeds a certain threshold value $thres_{black}$, X classifies Y as a black hole.

3.4. The GeoSec IRS

The *GeoSec* IRS excludes a detected black hole based on its location. If a node Y is classified as a black hole by the IDS of a node X, X obtains Y's location from the location service and establishes a quarantine zone with a radius d_{quar} around Y. As long as X is located within a quarantine zone, it will not forward any messages. All active routes which X is part of become invalid and the sources are informed appropriately. Since X will not forward any messages while it is located within a quarantine zone, subsequent route request messages will not reach the black hole Y, as shown in Figure 2. Thus, we prevent Y from being a part of newly established routes while it is quarantined. This approach is comparable to the restriction of broadcast messages as performed by LAR [13] and DREAM [14].

We assume that the position of a node is not observable within a quarantine zone. Therefore, updating the quarantine zone if Y moves is not possible. For this reason, a revocation of a quarantine zone is performed after a time t_{reset}.

By adapting the transmission power of nodes, we are able to decrease the radius d_{quar} of quarantine zones. In the following, we describe different strategies of how adaptive transmission power can be integrated. All calculations are based on a free space model. We assume

$$P_r(d) = P_s \cdot G_s \cdot G_r \cdot \frac{\lambda^2}{4 \cdot \pi^2 \cdot d^2}$$

In the formula, P_r denotes the signal strength in dB as it is received at the receiver r that is located in distance d from the sender s. P_r is subject to the transmission power P_s of the sender, the antenna gain G of sender and receiver, as well as to the wavelength λ of the signal. We assume that a signal can be received correctly if the received signal strength P_r is greater than a threshold P_{min}. We further assume that the antenna gain as well as P_{min} is the same for all nodes in the network. Please note that sender and receiver here refer to a physical layer transmission between adjacent nodes and not (necessarily) to the source and the destination of (multihop) routes on network layer.

3.4.1. Naïve GeoSec.

In the first version of *GeoSec*, no adaptive transmission power is used. Thus, the radius of a quarantine zone has to be set to at least the distance after which a signal can not be received correctly anymore. For the naïve GeoSec approach, d_{quar} is calculated as

$$d_{quar} = \sqrt{P_s \cdot G_s \cdot G_r \cdot \frac{\lambda^2}{4 \cdot \pi^2 \cdot P_{min}}}$$

To offer a security margin for node mobility, d_{quar} can be extended appropriately which will be subject of our evaluation.

3.4.2. GeoSec with Adaptive Transmision Power.

In theory it is possible to reduce transmission power such that a quarantine zone can be reduced to one single point in cartesian space. Still, it is reasonable to have a security margin for node mobility. Being given d_{quar} and the distance d_{center} from a node's location to the center of the closest quarantine zone, we can calculate P_s as

$$P_s(d_{center}) < \frac{P_{min}}{G_s \cdot G_r} \cdot \frac{4 \cdot \pi^2 \cdot (d_{center} - d_{quar})^2}{\lambda^2}$$

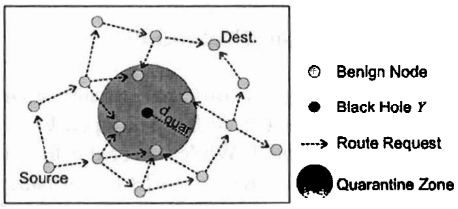
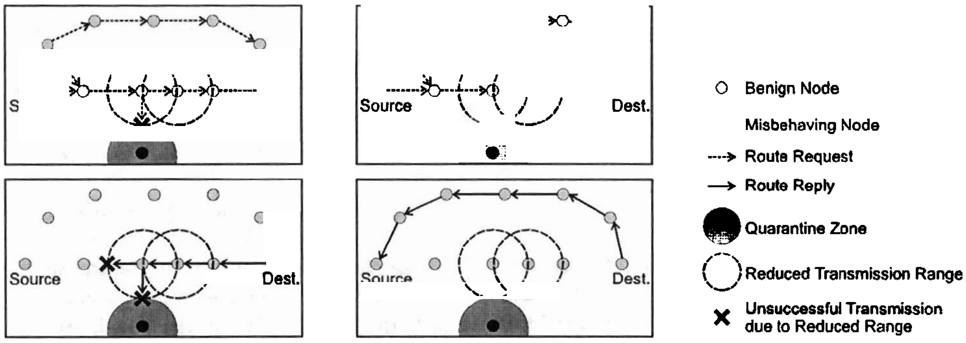


Figure 2. Restricted broadcast of route request messages due to *GeoSec*



(a) w/o asymmetry prevention

(b) With asymmetry prevention

Figure 3. Schematic representation of GeoSec with and without asymmetry prevention

3.4.3. GeoSec with Asymmetry Prevention. Assuming an 802.11 MAC protocol, we introduce asymmetric links between nodes by reducing the transmission power. While route request messages are sent as a broadcast without an RTS-CTS sequence that would prevent asymmetric links, route reply messages are sent as unicast messages. This may lead to scenarios where a node that operates with reduced transmission power is able to receive and forward a route request message, but will not be able to forward the corresponding route reply message. To prevent this, we further extended *GeoSec* such that a node that operates with reduced transmission power only forwards a route request message if the distance to the node from which it received the route request is less than d_{center}. Figure 3 depicts this situation. The upper figures show the dissemination of route request messages. The route reply phase is depicted in the lower figures.

4. Performance Evaluation

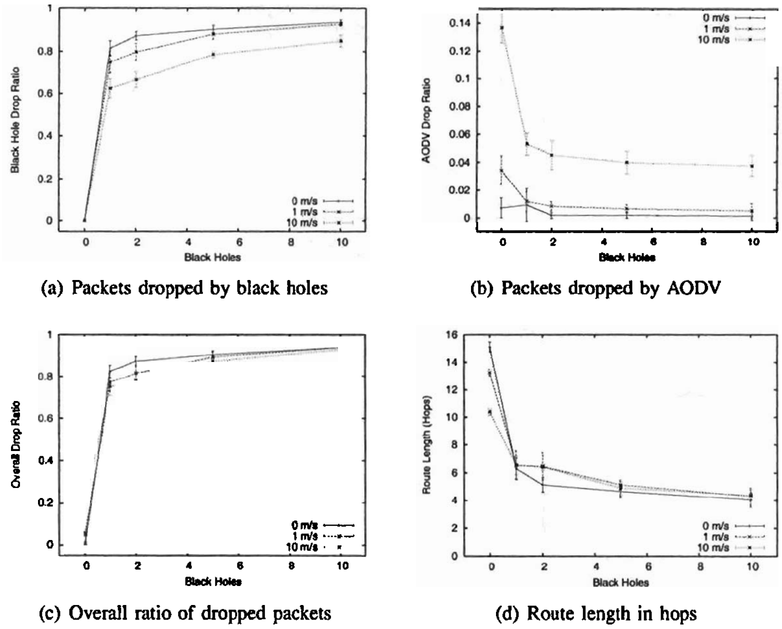
The goal of our evaluation is to compare the different strategies of adaptive transmission power with the naïve *GeoSec* approach. For this, we use an extended version of the JiST/SWANS [22] simulator. Besides other functionality, we added attack variants and the security mechanisms as presented in the previous section. To improve runtime, we use a Condor cluster [23] for distributed computation of the simulations.

4.1. Metrics Used for Evaluation

As metrics to compare the different variants of *GeoSec* we consider the packets that have been dropped by black hole nodes and by *GeoSec* itself. While our goal is to improve the latter, we do not want to degrade IRS performance subject to the first. We further consider packets dropped by the AODV routing protocol. This loss is caused by interrupted routes as well as by unreachable destinations (benign nodes located in quarantine zones). With this breakdown of the overall drop ratio, we are able to make clear assertions about the possibilities and limitations of the individual *GeoSec* variants.

4.2. Experimental Design

Benign nodes	990
Black holes	10
Antenna gain G	$0dB$
Transmission power P	$7dB$
Reception threshold P_{min}	$-81dB$
Signal wavelength λ	$2.4GHz$
Resulting transm. range	$\approx 250m$
Neighbors per node	7 - 8 (w/o adaptive power)
Resulting simulation area	4750 m · 4750 m
MAC Layer	IEEE 802.11 DCF with RTC/CTS
Network Layer	IPv4 with AODV routing service
Transport Layer	UDP
Traffic pattern	Constant bitrate traffic with 10 streams in parallel and a duration of 30 seconds per stream. Each stream transmits 4 packets per second with a size of 512 byte each. Sources and destinations are selected randomly.
Placement	Random placement (Uniform distribution of locations)
Mobility	Random waypoint, continuous movement
Simulated time	1 hour for each factor set split up in 6 runs with 10 minutes each



(a) Packets dropped by black holes

(b) Packets dropped by AODV

(c) Overall ratio of dropped packets

(d) Route length in hops

Figure 4. Effects of black holes in a network without security mechanisms

The basic network parameters listed above are chosen such that we obtain a moderate network load, i.e., the network operates in a non-congested state. Further, the density of the network has been chosen such that a connected (unpartitioned) network is typically achieved. The random waypoint mobility model can (compared to real-world scenarios) be considered as a worst-case scenario with respect to the predictability of node movement. The simulated time per factor set is split up in multiple simulation runs to reduce unwanted side-effects of the random waypoint model.

The factors that showed to have a considerable influence on our evaluation metrics are (1) the size of quarantine zones as defined by d_{quar} and (2) the velocity of nodes. The values used for our evaluation are chosen from the following sets. For each variant of *GeoSec*, we simulated all combinations of d_{quar} and the node velocity.

d_{quar}	0, 5, 15, 50 meters
Velocity	0, 1, 10 meters per second

In preliminary simulations, we adjusted the parameters of the IDS to achieve a reasonable performance with respect to true/false positives/negatives. We use $t_{mon} = 1second$, $w_{balance} = 10$, and $thres_{black} = 30$.

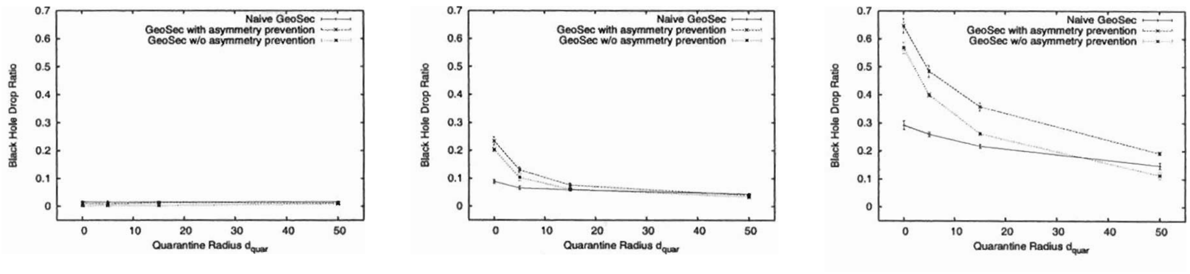
In addition, to show the effects of black hole attacks on a defenseless network, we simulated scenarios with 1, 2, 5, and 10 black holes for each level of node mobility considered.

4.3. Presentation of the Results

We now discuss the results of our simulation study starting with how black holes affect the performance of a defenseless network. Afterwards, we show to what extent *GeoSec* is able to recover the functionality of the network and to what extent an adaptive transmission power can act as a support. All plots are shown with 95% confidence intervals.

4.3.1. Black Holes in a Defenseless Network. Figure 4 shows how black holes affect the performance of a MANET without security measures. Regarding the metric of packets that are dropped by the black holes it stands out that one black hole in our scenario with 1000 nodes is sufficient to cause a ratio of packets dropped of more than 60%. The ratio of packets dropped by black holes raises to more than 80% for 10 black holes.

The black holes have a higher impact in scenarios with low node velocity. This can be explained with the help of the length of the routes that are established successfully. Also for scenarios without black hole nodes, the route length decreases if node velocity increases. Thus, the higher the velocity, the shorter the functional routes, the lower the probability for a black hole to be part of a route. The same reasoning holds for the fact that with an increasing number of black holes (and with increasing velocity), the ratio of packets dropped by AODV decrease. The shorter the routes, the lower the probability for route breaks.

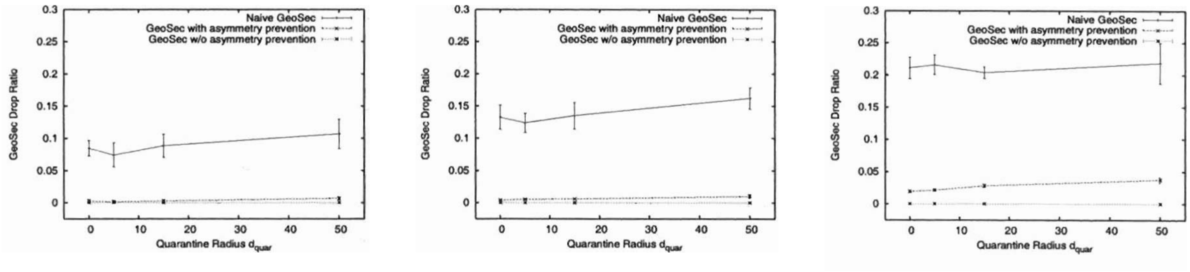


(a) Static nodes

(b) Mobile nodes; velocity 1 m/s

(c) Mobile nodes; velocity 10 m/s

Figure 5. Ratio of packets dropped by black holes



(a) Static nodes

(b) Mobile nodes; with 1 m/s

(c) Mobile nodes; with 10 m/s

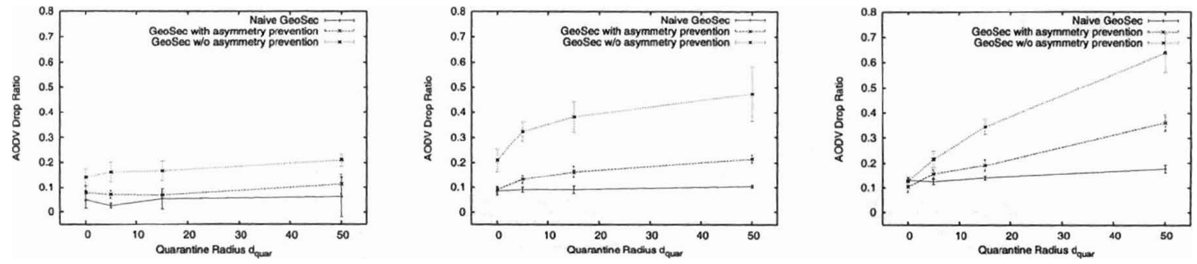
Figure 6. Ratio of packets dropped by GeoSec

4.3.2. Comparison of the Black Hole Drop Ratios. Figure 5 shows the ratio of packets dropped by black hole nodes subject to the different *GeoSec* variants and to the radius of quarantine zones d_{quar}. For static scenarios, we manage to reduce the black hole drop ratio from more than 90% in a defenseless network down to less than 2%. This holds for all schemes of *GeoSec* and can be understood as a proof of concept for the implementation. The remaining drops that are caused by black holes arise from the monitoring phase of the IDS during which packets still get dropped.

Since we assume that a black hole can not be tracked while it is quarantined, an adaptation of the quarantine zone if the black hole moves is not possible. Thus, if node velocity increases, the black holes leave the quarantine zones and can become active again. The greater the velocity, the faster this happens. Therefore, we obtain higher drop ratios caused by the black holes if we increase node velocity. For a velocity of 10 meters per second also the size of the quarantine zones has a remarkable influence. The larger the quarantine zone, the longer the quarantine zone is effective. Note that for the naïve *GeoSec* approach, d_{quar} is added to the 'standard' transmission range of 250 meters. As a whole, we can conclude that by using the power-adaptive strategies, we achieve drop ratios comparable to the naïve *GeoSec* approach for appropriate choices of the size of quarantine zones with respect to node velocity while being able to considerably reduce the size of the quarantine zones.

4.3.3. Comparison of the GeoSec Drop Ratios. The drop ratios that are caused by *GeoSec* itself are shown in Figure 6. The results show that with the power adaptive strategies we achieve our goal of reducing the drop ratio that is caused by *GeoSec* itself. Even for a high node velocity, we achieve drop ratios caused by *GeoSec* of less than 5% which can be accounted to the reduced size of the quarantine zones and, along with this, to the reduced number of affected benign nodes.

4.3.4. Comparison of the AODV Drop Ratios. Figure 7 shows the drop ratios that are induced by the AODV routing protocol. Here, clearly the drawbacks of an adaptive transmission power become obvious. Without an asymmetry prevention strategy, even for a low node velocity and static scenarios, the drop ratios that are caused by the routing protocol are intolerable. The effects that we depicted schematically in Figure 3 lead to drop ratios from 20% for static scenarios up to more than 60% in scenarios with a node velocity of 10 meters per second. Considerably better, but still worse results than for the naïve *GeoSec* approach can be achieved with the asymmetry-prevention strategy. We can conclude that a reduced transmission power leads to increased drop ratios due to broken routes since we have less room for node movement without leaving transmission ranges.

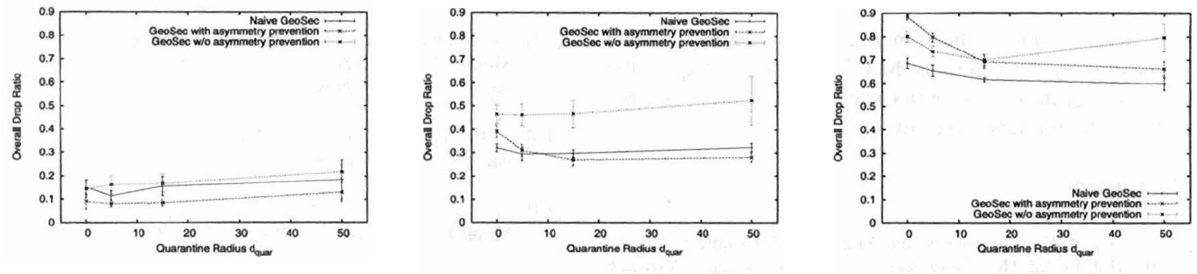


(a) Static nodes

(b) Mobile nodes; velocity 1 m/s

(c) Mobile nodes; velocity 10 m/s

Figure 7. Ratio of packets dropped by the AODV routing protocol



(a) Static nodes

(b) Mobile nodes; velocity 1 m/s

(c) Mobile nodes; velocity 10 m/s

Figure 8. Overall ratio of dropped packets

4.3.5. Comparison of the Overall Drop Ratios. The overall ratio of packets dropped is shown in Figure 8. Here, it gets obvious that the improvement of significantly reduced drop ratios due to the intrusion response is canceled out by the increased drop ratios caused by AODV. A minor overall improvement can be observed for a low velocity, if an adaptive power is used together with asymmetry prevention. Without asymmetry prevention, the adaptive power performs worse than the naïve *GeoSec* approach.

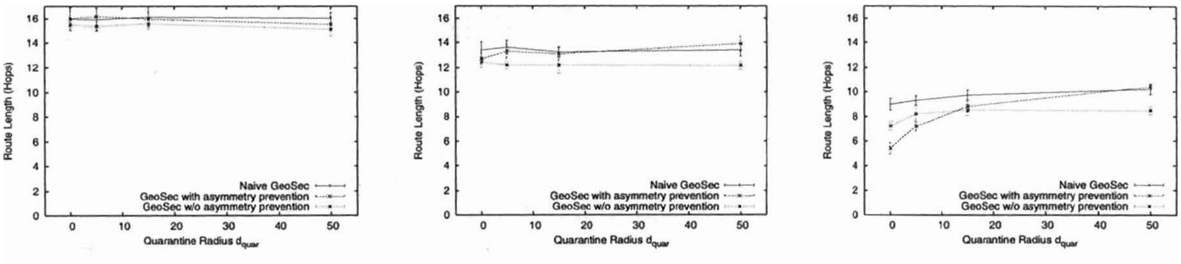
4.3.6. Comparison of the Route Length. Figure 9 shows how the length of the routes that have been established successfully is affected by the velocity of the nodes as well as by the different strategies of *GeoSec*. For all strategies the route length decreases when node velocity increases. This means that node mobility not only causes route breaks but also affects the route discovery process, which only takes a relatively short time. Obviously, during the time a route request is propagated to the destination until the route reply is sent back, the topology changes so rapidly that the path via which the route request had reached the destination is not available anymore. Regarding the different strategies of *GeoSec*, no considerable differences are observable. On the one hand, smaller quarantine zones lead to shorter routes in terms of the distance. On the other hand, a reduced transmission range leads to longer routes in terms of hops. As can be seen from Figure 9, these two factors that influence the route length seem to counterbalance each other. The power adaptive strategies tend to lead to shorter routes. This can be explained in analogy to the AODV drop ratios. The lower the transmission power, the faster the nodes move out of each other's transmission range.

5. Conclusion & Outlook

In this paper, we identified possibilities and limitations of supporting location-based intrusion response in MANETs by an adaptive transmission power. We proposed a simple power reduction scheme and a scheme that prevents effects of asymmetric links that arise when using a contention-based MAC protocol such as IEEE 802.11.

The evaluation showed that an adaptive power is able to considerably reduce unwanted side-effects of a location-based intrusion response. Still, the approach suffers from increased loss rates due to the (non power-aware) AODV routing protocol. We therefore plan to support our approach by power-aware routing protocols. We are further looking forward to go from simulation studies to testbed experiments. This way, we want to scrutinize the applicability of our approach in real-world scenarios.

We further plan to use the quality of experience of voice communication in MANETs as an additional metric for our evaluations. Voice communication, when appropriate codecs are used, can tolerate a high packet loss. Therefore it seems



(a) Static nodes

(b) Mobile nodes; velocity 1 m/s

(c) Mobile nodes; velocity 10 m/s

Figure 9. Route length in hops

to be a promising application that can inherently handle the challenging conditions in MANETs while fitting to the envisioned application scenarios such as emergency response or police and military operations.

References

[1] B. Wu et al., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in *Wireless/Mobile Network Security*, Springer, 2006.

[2] D. Djenouri et al., "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Comm. Surveys & Tutorials*, vol. 7, 2005.

[3] M. G. Zapata et al., "Securing Ad hoc Routing Protocols," in *Proc. of WiSE '02.*

[4] Y. C. Hu et al., "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in *Proc. of MobiCom '02.*

[5] Y. C. Hu et al., "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proc. of WiSe '03.*

[6] G. Acs et al., "Provable Security of On-Demand Distance Vector Routing in Wireless Ad Hoc Networks," in *Proc. of ESAS '05.*

[7] G. Acs et al., "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1533–1546, 2006.

[8] S. Buchegger, "Coping with Misbehavior in Mobile Ad-hoc Networks," Ph.D. dissertation, École Polytechnique Fédérale de Lausanne, 2004.

[9] P. Michiardi et al., "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in *Proc. of the Sixth Joint Working Conf. on Comm. and Multimedia Security*, 2002.

[10] S. Bansal et al., "Observation-based Cooperation Enforcement in Ad hoc Networks," Stanford University, Tech. Rep., July 2003.

[11] A. König et al., "GeoSec - Quarantine Zones for Mobile Ad Hoc Networks, in *Wiley Journal on Security and Communication Networks*, to appear.

[12] M. Mauve et al., "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," *IEEE Network Magazine*, vol. 15, no. 6, pp. 30–39, November 2001.

[13] Y.-B. Ko et al., "Location-Aided Routing (LAR) in Mobile Ad Hoc Networks," in *Proc. of MobiCom '98.*

[14] S. Basagni et al., "A Distance Routing Effect Algorithm for Mobility (DREAM)," in *Proc. of MobiCom '98.*

[15] I. A. Getting, "The Global Positioning System," *IEEE Spectrum*, vol. 30, no. 12, pp. 36–38, 43–47, December 1993.

[16] A. Srinivasan et al., "A Survey on Secure Localization in Wireless Sensor Networks," in *Encyclopedia of Wireless and Mobile Communications*, CRC Press, 2007.

[17] S. Singh et al., "Power-Aware Routing in Mobile Ad Hoc Networks," in *Proc. of MobiCom '98.*

[18] R. Ramanathan et al., "Topology Control of Multihop Wireless Networks using Transmit Power Adjustment," in *Proc. of INFOCOM 2000.*

[19] D. M. Blough et al., "The K-Neigh Protocol for Symmetric Topology Control in Ad Hoc Networks," in *Proc. of MobiHoc '03.*

[20] S.-J. Park et al., "Load-Sensitive Transmission Power Control in Wireless Ad-hoc Networks," in *Proc. of GLOBECOM '02.*

[21] I. Siomina et al., "Maximizing Lifetime of Broadcasting in Ad Hoc Networks by Distributed Transmission Power Adjustment," in *Proc. of ICTON '06.*

[22] R. Barr, "An Efficient, Unifying Approach to Simulation using Virtual Machines," Ph.D. dissertation, Cornell University, 2004.

[23] Department of Computer Science, University of Wisconsin - Madison, "Condor Project Homepage," *http://www.cs.wisc.edu/condor.*