An Analytical Model of Routing, Misbehavior, and Countermeasures in Mobile Ad Hoc Networks

André König, Daniel Seither, Ralf Steinmetz
Multimedia Communications Lab
Technische Universität Darmstadt
{andre.koenig, daniel.seither, ralf.steinmetz}@kom.tu-darmstadt.de

Matthias Hollick
Center for Advanced Security Research Darmstadt
Technische Universität Darmstadt
matthias.hollick@cased.de

***Abstract*—We present an analytical model combining geometric and stochastic approaches to describe the effects of attacks and countermeasures on MANETs. In particular, we focus on the packet loss that can be charged to the misbehavior as well as to the countermeasures as a primary metric. For this, we model the entire chain of (1) MANET routing, (2) attack, (3) intrusion detection, and (4) intrusion response. We validate the models proposed by means of simulation.**

I. Introduction

Conditions such as wireless data transmission and lack of a communication infrastructure turn mobile ad hoc networks (MANET) into a challenging environment from the perspective of security. Various kinds of misbehavior were identified e.g. in [1] and in [2]. To face these, preventive as well as reactive security measures that are tailored to the conditions in MANETs were proposed. Well known preventive security mechanisms are secure routing protocols such as SAODV [3] or Ariadne [4]. Based on means of cryptography, these protocols were designed to prevent false routing information from being injected into the network as well as correct routing information from being tampered with. Though designed meticulously, attack vectors for both protocols were found recently in [5]–[7]. For the case of compromised preventive security mechanisms, reactive measures can be taken to establish a second line of defense. In general, this is done by intrusion detection systems (IDS) combined with intrusion response systems (IRS).

IDSs for MANETs are well investigated; for survey information we refer to [8]. Yet, only sparse attention has been paid to how to react to intrusions detected. In most IRS schemes, e.g. in [9]–[11], an address-based response is performed. Here, a misbehaving node is identified by its (network) address and transmissions to/from this address are blocked. Since nodes in a MANET are beyond the control of a central instance, changing addresses is possible with little effort. Therefore, an address-based IRS may have significant drawbacks when deployed in MANETs. As an alternative, we proposed a location-based IRS in [12]. Here, to exclude a misbehaving node from the network, a geographic quarantine zone is established around the node's location. Transmissions into or out of a quarantine zone are blocked. Thus, as shown in Figure 1, routes in the MANET are established bypassing quarantine zones. This way, communication is kept away physically from areas affected by misbehavior.

In [12] we compared the performance of the location-based IRS with an address-based solution when confronted with a combination of a black hole and a Sybil attack. Based on simulation studies for selected scenarios, we showed that a location-based IRS may perform better than an address-based approach. Yet, in general, this trade-off depends on various factors such as the particular configuration of the MANET, of the attack mechanisms, and of the IDS as well as of the IRS. Since this parameter space is too large to be scrutinized completely by means of simulation (or in testbeds), we propose a generalized analytical model of the attack mechanism and of the IRS in this paper. With this, we obtain a more comprehensive view on the system. We focus on modeling the packet loss that is caused by misbehaving nodes as well as by the countermeasures deployed. For this, we follow an elementary approach based on a combined geometric and stochastic description of the routing protocol and of the location-based IRS. By reducing complexity this way, we obtain a straightforward description of the system allowing for comprehensible insights.

After presenting related work on analytical models for MANETs in the following section, we briefly describe the relevant details of the routing protocol and of the location-based IRS in Section III. We then develop the analytical model in Section IV. A comparison of the model predictions with simulation results in Section V concludes this paper.

II. Related Work

A metric that was often described analytically is the throughput of MANETs. One of the first models for this is presented in [13]. The authors develop an upper bound for the per node throughput subject to the total number of nodes in the MANET and to the theoretical transmission speed of the network. [13] served as basis for several further studies on the throughput of MANETs. In [14], the influence of the

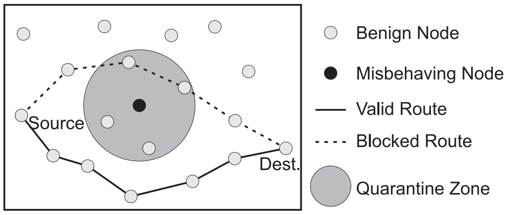


Fig. 1. Schematic representation of the location-based IRS

transmission range on the upper bound proposed in [13] is described. An analysis of the effect of different traffic patterns is performed in [15]. The impact of node mobility is described in [16].

The end-to-end delay in MANETs subject to the number of nodes and to node mobility is modeled in [17]. Closely related to the delay are the length (geographical distance of sender and receiver) and the lifetime (time until nodes move out of each others transmission range) of single-hop links and multi-hop routes. A model for the length of single-hop links for a uniform as well as for a Gaussian distribution of node locations is proposed in [18]. The route length for a uniform node distribution is described in [19]. The lifetime of single-hop links subject to node mobility is analyzed in [20]. In [21], analytical models for the lifetime of multi-hop routes are developed for different mobility models.

To the best of our knowledge, [19] is the only work that describes the effects of node misbehavior in MANETs by means of a geographical model. However, it focuses on the route-length distribution as a metric only and does neither include modeling of packet loss nor of security mechanisms.

III. Architecture

In this section we describe the MANET routing, the attack mechanisms, the IDS, and the IRS. We consider a reactive routing protocol that selects routes based on age and a distance metric, and uses an expanding ring search in order to reduce the network load. We exemplify this routing behavior using the AODV protocol [22].

A. The Routing Protocol

Reactive routing protocols establish a route between a source and a destination not unless a transmission should happen. In this case, AODV starts a route discovery process initiated by the source by sending a route request (RREQ) message for the intended destination. The RREQ is disseminated as a broadcast. Upon receiving a RREQ at the destination node, a route reply (RREP) message is sent back to the source. In case of receiving multiple RREPs for the same destination, AODV chooses the most recent (determined by a sequence number) and shortest (determined by a hop count) route, whereas newer routes are preferred over shorter ones.

Since disseminating RREQs as broadcast messages causes a high network load, AODV may use an expanding ring search to mitigate this effect. [22] proposes to search routes consecutively in the 1-, 2-, 3-, 5-, and 7-hop neighborhood of the source. If a route is not found in these steps, the search is extended to the full network diameter which is assumed to be 35 hops in [22].

B. The Black Hole Attack

Comparable to the effect of a black hole in terms of astronomy, a black hole in a MANET attracts and 'absorbs' network traffic. For attacking AODV, this is done by issuing RREP messages with falsified age and/or distance metrics. To obtain a worst-case behavior, we consider a black hole that eavesdrops sequence numbers and answers every RREQ received with the current sequence number of the intended destination incremented by one and a hop count set to one (regardless of whether the intended destination really is a neighbor of the black hole). With this, the route that is offered by the black hole appears to be both newer and shorter than the route that is offered by the real destination. Thus, the route offered by the black hole is selected by the source according to the specification of AODV. To complete the 'absorbing' effect, the black hole does not forward any data packets after the route is established.

C. The IDS

We model a generalized IDS that, similar to OCEAN [11], works based on local (per node) 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 located within the transmission range of X). For each of its neighbors, X maintains a counter n_{rec} for packets that Y 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 describing the forwarding behavior of each of its neighbors. R_Y is defined as

$$R_Y \quad = \quad R'_Y \cdot \frac{n_{rec}}{w_{bal}} - n_{forw}$$

In this definition R'_Y denotes the rating of the previous monitoring interval and $w_{bal} \geq 1$ is a weighting factor to balance n_{rec} and n_{forw}. If R_Y exceeds a threshold $thres_{black}$, X classifies Y as a black hole.

D. The Location-based IRS

If a node Y is classified as a black hole by the IDS of a node X, X establishes a quarantine zone with a radius r_{quar} around Y. As long as X is located within this quarantine zone, it will not forward any messages. All active routes which X is part of become invalid. Since X will not forward any messages while it is located in 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.

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 quarantine zones is performed after the interval t_{reset}.

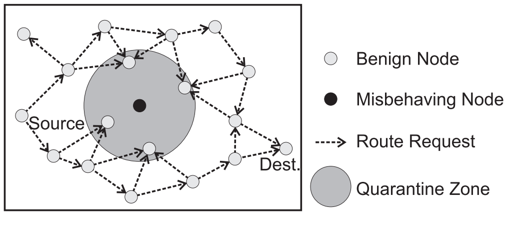


Fig. 2. Mode of operation of the location-based IRS

NOTATIONS OF FORMULAE

t_{mon}	Monitoring interval of the IDS in seconds
n_{rec}	Number of packets a node received during t_{mon}
n_{forw}	Number of packets a node forwarded during t_{mon}
w_{bal}	Factor to balance n_{rec} and n_{forw}
R_Y	Rating for node Y determined by the IDS
$thres_{black}$	Threshold of R_Y for classification as black hole
r_{quar}	Radius of quarantine zones
t_{detect}	Time needed to detect a black hole
t_{reset}	Time after which quarantine zones are revoked
r_{trans}	Transmission range of nodes
A_{net}	Size of the network
l	Side length of the network area
d_{hop}	Average distance per hop
n_{total}	Total number of nodes in the network
n_{black}	Number of black hole nodes in the network
n_s	Number of nodes reached in Step s of the ring search
ρ	Network density in nodes per area

IV. The Model

Within this section we develop the analytical model describing the effects of the black hole attack and of the location-based IRS on the packet loss experienced in the MANET. After defining basic assumptions we start with modeling the expanding ring search behavior of the routing protocol which leads to the probability for a black hole being included in a route. Based on this, we describe the packet loss that can be charged to black holes in a MANET without intrusion detection and response. We continue with modeling the packet loss caused by black holes with activated IDS/IRS subject to the time the IDS requires to detect a black hole and to the mobility of nodes. A model for the packet loss caused by the IRS itself concludes this section.

A. Assumptions

In the following, we assume

- a square network area A_{net} with side length l
- a circular transmission area with radius r_{trans},
- quarantine zones to match the transmission area of the corresponding misbehaving node at the time the quarantine zone is established,
- a geometrically uniform distribution of benign nodes and black holes within the network area,
- randomly selected sources and destinations of traffic,
- a random distribution of traffic patterns among all nodes, i.e., the network load is constant and nodes can not be distinguished by their communication,
- a connected network, i.e., a route between any two nodes can be established at any time.

B. Expanding Ring Search

For modeling the packet loss, we need to describe the expanding ring search in terms of the number of new nodes a RREQ message reaches in each step as shown in Figure 3. For this, let A_h be the circular area covering all nodes located in a distance of at most h hops to the source of the RREQ, where $A_0 = 0$ and $\Delta A_h = A_h - A_{h-1}$. Depending on the actual network configuration, a fix average geometric per-hop routing progress $0 < d_{hop} < r_{trans}$ can be assumed. For the remainder of this paper, we use $d_{hop} = \frac{r_{trans}}{\sqrt{2}}$, which was obtained experimentally in [19] for a realistic MANET configuration. This leads to a first estimate of ΔA_h defined as

$$\begin{aligned}\Delta\Lambda_h &= \Lambda_h - \Lambda_{h-1} = \pi(h \cdot d_{hop})^2 - \pi((h-1)d_{hop})^2 \\ &= (2h-1)\pi \cdot d_{hop}^2\end{aligned}$$

This description holds if the ring search does not leave the simulation area. To include edge effects for nodes being located at the borders of the simulation area we use a four-step approximation. For a ring radius $r = h \cdot d_{hop} < \frac{l}{2}$ of less than half the side length l of the simulation area, the ring can be contained fully in the simulation area in the best case for a node being located at the center. In the worst case, for a node being located at a corner, only one quarter of the ring reaches into the simulation area. Since nodes are assumed to be distributed uniformly, both cases and any in between are equally likely. Thus, for $r = h \cdot d_{hop} < \frac{l}{2}$ we obtain $\Delta A_h = \frac{1}{2}\left(\Lambda_h + \frac{1}{4}\Lambda_h\right)$. In analogy, we approximate the cases for a ring radius between half side length and side length, between side length and diagonal length, and larger than diagonal length. Altogether, we obtain

$$\Delta A_h = \begin{cases} \frac{1}{2}\left(\Lambda_h + \frac{1}{4}\Lambda_h\right) & \text{if } h \cdot d_{hop} \le \frac{l}{2} \\ \frac{1}{8}\Lambda_h & \text{if } \frac{l}{2} < h \cdot d_{hop} \le l \\ \frac{1}{16}\Lambda_h & \text{if } l < h \cdot d_{hop} \le \sqrt{2l^2} \\ 0 & \text{otherwise} \end{cases}$$

As described in Section III-A, the expanding ring search is performed in consecutive steps in each of which the TTL of a RREQ is incremented. Let h_s be the TTL in hops for Step s. With the default parameters specified in [22], h_s is given by the following table (we set $h_0 = 0$ for reasons of simplification).

s	0	1	2	3	4	5
h_s	0	1	3	5	7	35

For the description of the number n_s of nodes that are reached in Step s of the expanding ring search let n_{total} be the total number of nodes and A_{net} be the total area of the network. Because nodes are assumed to be distributed uniformly, the geometric density of nodes is given by $\rho = \frac{n_{total}}{A_{net}}$. We get

$$\begin{aligned} n_0 &= 0 \\ n_s &= n_{s-1} + \Delta n_s \text{ where } \Delta n_s = \sum_{i=h_{s-1}+1}^{h_s} \Delta A_i \cdot \rho \end{aligned}$$

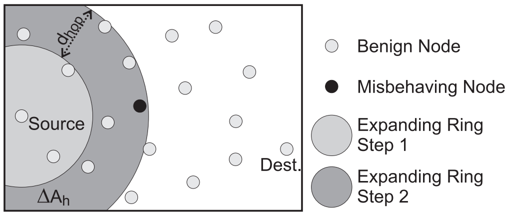


Fig. 3. Area covered by expanding ring search subject to d_{hop}

C. Packet Loss due to Black Holes in a Defenseless MANET

To model the packet loss caused by black holes, we start with describing the probability $p_{black}(s)$ for a RREQ reaching at least one black hole until Step s of the expanding ring search. If we assume n_{black} black holes in n_{total} total nodes, we have $n_{total} - n_{black}$ benign nodes in the network. Thus, the number of possible combinations to select the n_s nodes that are reached in Step s of the ring search only from benign nodes is $x = \binom{n_{total}-n_{black}}{n_s}$. The number of combinations for selecting the n_s nodes from n_{total} total nodes is $y = \binom{n_{total}}{n_s}$. Now, $\frac{x}{y}$ describes the probability that a RREQ reaches only benign nodes until Step s of the ring search. For the probability $p_{black}(s)$ that a RREQ reaches at least one black hole until Step s of the ring search, we have to consider the special case of $n_s > n_{total} - n_{black}$, i.e., the number of nodes reached in Step s exceeds the number of benign nodes. Certainly, the RREQ reaches a black hole in this case. Altogether, we get

$$p_{black}(s) \quad = \quad \begin{cases} 1 & \text{if } n_s > n_{total} - n_{black} \\ 1 - \frac{\binom{n_{total}-n_{black}}{n_s}}{\binom{n_{total}}{n_s}} & \text{otherwise} \end{cases}$$

We assume a random selection of traffic patterns as well as of source and destination nodes. Hence, the probability for a data packet to get lost due to a black hole equals the probability for a black hole being part of the corresponding route between source and destination. To determine this, we need to calculate the probability $p_{dest}(s)$ for reaching the destination node in Step s of the ring search. Since destinations are assumed to be chosen randomly, this probability correlates to Δn_s. We obtain $p_{dest}(s) = \frac{\Delta n_s}{n_{total}}$. With this, the probability for the RREQ reaching the destination in Step s and at least one black hole until Step s of the ring search is given by $p_{dest}(s) \cdot p_{black}(s)$. For the overall probability $p_{loss,black}$ for data packets to get lost due to a black hole we need to consider all steps of the expanding ring search. We get

$$p_{loss,black} \quad = \quad \sum_{i=1}^{5} p_{dest}(i) \cdot p_{black}(i)$$

D. Packet Loss due to Black Holes with IDS/IRS

Although the location-based IRS excludes black hole nodes from the network, the influence of black holes can only be mitigated and not be thwarted completely. Thus, the probability $p_{loss,defended}$ for packet loss despite active security measures can be described as

$$p_{loss,defended} \quad = \quad p_{loss,black} \cdot p_{IRSfail}$$

Here, $p_{IRSfail}$ denotes the probability that the IRS fails to prevent a black hole from dropping packets. As the main influences on $p_{IRSfail}$ we identified the detection time of the IDS and the mobility of nodes. Both lead to independent parts $p_{IRSfail,detect}$ and $p_{IRSfail,move}$ of $p_{IRSfail}$. Thus, we obtain

$$p_{IRSfail} \quad = \quad p_{IRSfail,detect} + p_{IRSfail,move}$$

1) Impact of the IDS: To detect misbehavior ongoing an IDS has to monitor the suspicious node for a certain time. In our scenario, the black hole may continue dropping packets during this time. To describe the resulting probability $p_{IRSfail,detect}$ (as a part of $p_{IRSfail}$) for packet loss during the time the IDS needs to identify misbehavior, we start by modeling the detection time. For our IDS as introduced in Section III-C, the detection time is given as $t_{detect} = n_{mon} \cdot t_{mon}$ where n_{mon} denotes the number of monitoring intervals needed until a black hole is detected and t_{mon} denotes the duration of a monitoring interval.

As described, a node Y is classified as a black hole, if the rating r_Y exceeds the threshold $thres_{black}$. Since a black hole node in our case does not forward any packets, R_Y is defined as $R_Y = \frac{n_{rec}}{w_{bal}}$ per monitoring interval t_{mon}. If we consider a steadily loaded network, the traffic during the detection time is (nearly) constant at a rate λ. Thus, $n_{rec} = \lambda \cdot t_{mon}$. If a black hole is detected, $n_{mon} \cdot \frac{\lambda \cdot t_{mon}}{w_{bal}} > thres_{black}$ holds. The number n_{mon} of monitoring intervals needed to detect a black hole is then given by $n_{mon} = \frac{thres_{black} \cdot w_{bal}}{\lambda \cdot t_{mon}}$. Thus, for the detection time of the IDS we obtain

$$t_{detect} \quad = \quad \frac{thres_{black} \cdot w_{bal}}{\lambda}$$

After a black hole was detected, the corresponding quarantine zone excludes the black hole from the network for the time t_{reset}. Altogether, a black hole can be active for the time t_{detect} as part of the total detection-protection-period $t_{detect} + t_{reset}$. Thus, for the probability $p_{IRSfail,detect}$ of losing packets due to n_{black} black holes during the detection time of the IDS we obtain

$$p_{IRSfail,detect} \quad = \quad n_{black} \cdot \frac{t_{detect}}{t_{detect} + t_{reset}}$$

2) Impact of Node Mobility: We assume that quarantine zones can not be adapted directly when a node moves, since an observation is not possible when a node is quarantined. Thus, as shown in Figure 4, mobility of a black hole leads to a new affected area A_{affect}. Nodes in this area are not aware of the black hole and will forward RREQ messages without restrictions.

The probability $p_{IRSfail,move}$ for packet loss due to node mobility can be modeled based on the number n_{affect} of nodes located in A_{affect}. Each of these nodes has to perform a detection of the black hole leading to a corresponding multiple of $p_{IRSfail,detect}$ as described in the previous section.

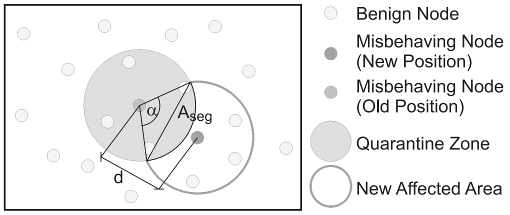

α
A_seg
d
Benign Node
Misbehaving Node (New Position)
Misbehaving Node (Old Position)
Quarantine Zone
New Affected Area

Fig. 4. Influence of black hole mobility on the IRS

The angle α, as shown in Figure 4, can be determined by $\alpha = 2 \cdot \arccos\left(\frac{d}{2r_{trans}}\right)$ where d denotes the distance between the position where the black hole was first detected and its new location. With this, we can determine the area A_{seg} of the circular segment defined by the quarantine zone and A_{affect}. We get $A_{seg} = \frac{r_{trans}^2}{2} \cdot (\alpha - \sin(\alpha))$, thus

$$A_{affect} \quad = \quad \pi r_{trans}^2 - 2 \cdot A_{seg}$$

Since the nodes are distributed uniformly within the network area we get $n_{affect} = A_{affect} \cdot \rho$. Thus, the loss due to node mobility can be described as

$$p_{IRSfail,move} \quad = \quad n_{affect} \cdot n_{black} \cdot p_{IRSfail,detect}$$

E. Packet Loss due to the IRS

Packet loss due to the IRS arises from (benign) nodes located in quarantine zones being source or destination of a communication. To model the probability $p_{loss,IRS}$ for packet loss due to the IRS, we thus have to determine the number of nodes that is located in quarantine zones.

To calculate the total area $A_{quar}(n_{black})$ that is covered by quarantine zones, we use a simple heuristic for the probability $p_{lap}(n_{black})$ that quarantine zones overlap. This is the case if two black holes are located closer than $2 \cdot r_{trans}$. We define

$$\begin{aligned} p_{lap}(1) &= 0 \\ p_{lap}(i) &= \frac{A_{lap}(i-1)}{A_{net}} \text{ if } i > 1 \end{aligned}$$

The areas $A_{lap}(n_{black})$ that are needed to determine $p_{lap}(n_{black})$ are defined as

$$\begin{aligned} A_{lap}(1) &= \pi \cdot (2 \cdot r_{trans})^2 \\ A_{lap}(i) &= A_{lap}(i-1) + (1 - p_{lap}(i)) \cdot \pi(2 \cdot r_{trans})^2 \\ &\quad \text{if } i > 1 \end{aligned}$$

With this, $A_{quar}(n_{black})$ can be calculated as

$$\begin{aligned} A_{quar}(1) &= \pi \cdot r_{trans} \\ A_{quar}(i) &= A_{quar}(i-1) + \pi r_{trans}^2 \cdot (1 - p_{lap}(i)) \\ &\quad \text{if } i > 1 \end{aligned}$$

To determine $p_{loss,IRS}$ we now have to describe the probability of either source or destination or both nodes being located within a quarantine zone. Since nodes are distributed uniformly, the probability that an arbitrarily chosen node is available (i.e., not quarantined) is given as

$$p_{avail} \quad = \quad 1 - \frac{A_{quar}(n_{black})}{A_{net}}$$

The probability that both source and destination are available is p_{avail}^2. Thus, we obtain

$$p_{loss,IRS} \quad = \quad 1 - p_{avail}^2$$

TABLE I
COMPARISON OF MODEL PREDICTIONS AND SIMULATION RESULTS FOR THE PACKET LOSS DUE TO BLACK HOLES IN A DEFENSELESS NETWORK

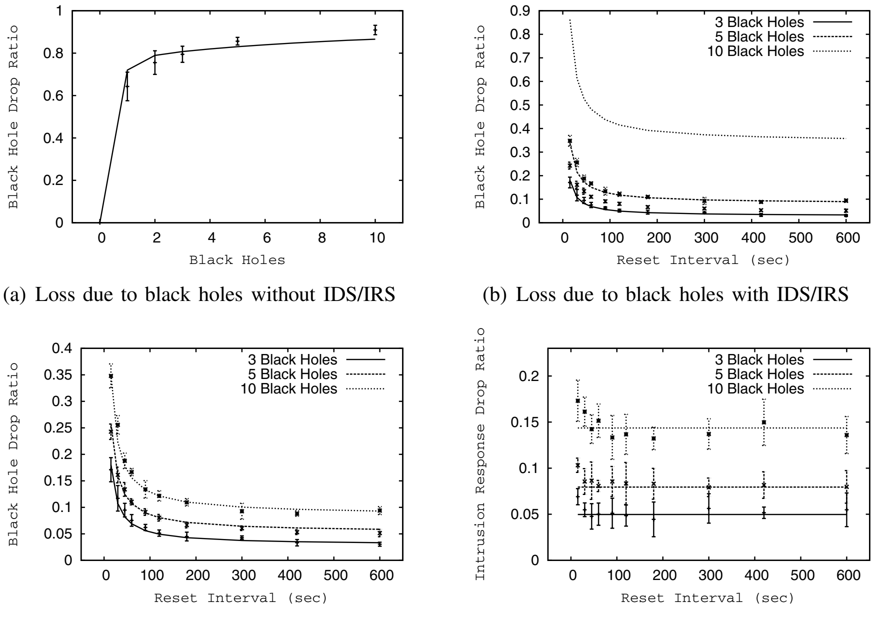
n_{black}	model prediction x	sim. result y	sim. conf. z	$x - y$	$\frac{x-y}{z}$
1	0.720	0.643	0.067	0.077	1.144
2	0.789	0.755	0.056	0.034	0.611
3	0.807	0.795	0.038	0.013	0.334
5	0.830	0.856	0.018	-0.026	-1.454
10	0.866	0.909	0.022	-0.043	-1.964

V. MODEL VALIDATION

To validate our work, we compare the model predictions with the results of the simulation study we presented in [12]. To visually demonstrate the accuracy achieved, we show the model predictions as curves together with the 95% confidence bars taken from the simulation results in Figure 5. The simulation results were obtained from a scenario consisting of $n_{total} = 1000$ nodes with $n_{black} \in \{1, 2, 3, 5, 10\}$ black holes on a square simulation area A_{net} with $l = 4750m$ side length. The nodes moved continuously according to a random waypoint mobility model (which can be considered as a worst-case scenario regarding predictability) with a speed between 1 and 2 meters per second. This leads to an average distance $d = \frac{t_{reset} \cdot \text{meters}}{6 \cdot \text{second}}$ from the location at which a black hole was detected to its new location when the quarantine zone is revoked. We used a constant bitrate traffic pattern with a network load of 20 streams in parallel consisting of packets with a size of 512 byte at a rate of 2048 kbytes per second. With a detection threshold $thres_{black} = 10$ determined as an optimum in preliminary simulations for the scenario given, the resulting detection time of the IDS is $t_{detect} = 1s$. The reset intervals for quarantine zones were taken from $t_{reset} \in \{15, 30, 45, 60, 90, 120, 180, 300, 420, 600\}$ in seconds. Each scenario was simulated for one hour simulated time split up in 6 parts of 10 minutes each to reduce side effects of the random waypoint mobility model.

The comparison for the loss caused by black holes in a defenseless network is shown in Figure 5(a). For the 2, 3, and 5 black hole scenarios, the model prediction is within the confidence interval of the simulation results. The small deviation for the setups with 1 and 10 black holes can be explained by the inaccuracy of the heuristic we used to model edge effects of the expanding ring search. Yet, the error of the model prediction is alway less than two times the simulation confidence as shown in Table I.

Figure 5(b) shows the comparison for the loss caused by black holes in a network with IDS/IRS. Please note that for reasons of readability only the results for the 3, 5, and 10 black hole scenarios are presented. While prediction and confidence intervals (i.e. simulation results) match well for the 1, 2, and 3 black hole scenarios, it stands out that for the 5 and 10 black hole setups the prediction and the simulation results differ strongly (note that the curve matching the 10 black hole confidence bars belongs to the 5 black hole prediction). Rerunning and tracing the simulations, we found that in the scenario with 5 black holes only 4 and in the scenario with



(a) Loss due to black holes without IDS/IRS

(b) Loss due to black holes with IDS/IRS

(c) (b) adapted to black hole activity

(d) Loss due to IRS

Fig. 5. Comparison of model predictions (curves) and simulation results (confidence bars)

10 black holes only 5 are active at the same time. We put this down to the overlapping-effects of quarantine zones and effects of black holes located at the edges of the simulated area. A detailed investigation of this point is part of our future research. If we instantiate the model accordingly (4 / 10 black holes in the model for the 5 / 10 black hole simulation setups), we obtain a match for all scenarios as shown in Figure 5(c).

The comparison for the loss that is caused by the IRS itself is shown in Figure 5(d). Again, we obtain a reasonable match of model and simulation. Yet, in this case the simulation results show significant variances. This is due to false positives of the IDS and also part of our future work.

VI. Conclusion & Outlook

In this paper, we developed an analytical model that describes the effects of black hole attacks and of location-based countermeasures on MANETs. Based on a combined geometric and stochastic approach, we developed a light-weight model for the routing process as well as for the packet loss caused by the misbehavior and by the countermeasures. The comparison of the model and of simulation results show that the model developed produces reasonable predictions despite following an elementary approach.

In future work we plan to improve the model by developing more precise descriptions of edge effects on the expanding ring search and on black hole activity. We further plan to model the trade off between location-based and address-based intrusion response which was not subject of this paper.

References

[1] B. Wu et al., “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks,” in *Wireless/Mobile Network Security*, ser. Network Theory and Applications. Springer, 2006, vol. 17, ch. 12.

[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 TMC*, vol. 5, no. 11, 2006.

[8] T. Anantvalee et al., “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in *Wireless Network Security*, ser. Signals and Communication Technology. Springer US, 2007.

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

[10] 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.

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

[12] A. König et al., “GeoSec: quarantine zones for mobile ad hoc networks,” *Security and Communication Networks (Wiley SCN)*, Online, 2008.

[13] P. Gupta et al., “The Capacity of Wireless Networks,” *IEEE Transactions on Information Theory*, vol. 46, no. 2, 2000.

[14] E. Kail et al., “The Effect of the Transmission Range on the Capacity of Ideal Ad Hoc Networks,” in *Proc. of WPMC’01*.

[15] J. Li et al., “Capacity of Ad Hoc Wireless Networks,” in *Proc. of MobiCom ’01*.

[16] M. Grossglauser et al., “Mobility Increases the Capacity of Ad-hoc Wireless Networks,” *IEEE/ACM TON*, vol. 10, no. 4, 2002.

[17] R. Groenevelt et al., “Message Delay in MANET,” in *Proc. of SIGMETRICS’05*.

[18] L. E. Miller, “Distribution of Link Distances in a Wireless Network,” *NIST Journal of Research*, vol. 106, no. 2, 2001.

[19] M. Hollick, “Dependable Routing for Cellular and Ad hoc Networks,” Ph.D. dissertation, Technische Universität Darmstadt, 2004.

[20] P. Samar et al., “On the Behavior of Communication Links of a Node in a Multi-Hop Mobile Environment,” in *Proc. of MobiHoc’04*.

[21] F. Bai et al., “Modeling Path Duration Distributions in MANETs and their Impact on Reactive Routing Protocols,” *IEEE JSAC*, vol. 22, no. 7, pp. 1357–1373, September 2004.

[22] C. E. Perkins et al., “Ad hoc On-Demand Distance Vector (AODV) Routing,” *IETF RFC 3561*, 2004.