

Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networks

Malcolm Parsons
Interactive Graphics Systems Group
Technische Universität Darmstadt
Fraunhoferstr. 5, 64283 Darmstadt, Germany
malcolm.parsons@gmx.de

Peter Ebinger
Security Technology Department
Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstr. 5, 64283 Darmstadt, Germany
peter.ebinger@igd.fraunhofer.de

Abstract—The rise in research on and use of Mobile Ad hoc Networks (MANETs) has seen an equal increase in the number of attack strategies, detection methods and counter measures proposed. Most of these have been analyzed and evaluated in separate simulation experiments according to performance metrics chosen for a specific purpose, however, simulation results are not comparable due to varying evaluation scenarios and implementations.

In this paper we implement and evaluate the most prominent attacks described in literature in a consistent manner to provide a concise comparison on attack types and parameters. Our objective is to thoroughly capture and analyze the impact of a range of attacks on MANET performance. To this end we define performance metrics and explore influence and damage caused by several attack types and parameter sets.

Our evaluation results show that the degree of impact of attacks differs significantly depending on attack type and parameters used. The impact of a particular attack increases considerably with an increasing number of attacking nodes in several of the scenarios, whereas other attack impact levels remain almost constant with varying number of attackers. These results imply that an attacker could choose an attack strategy from a number of alternatives with similar overall impact thereby minimizing detection risk. Our performance metrics provide a consistent comparison of various attack types and parameters and thus a deeper insight into the interaction and the impact of attacks in MANETs.

Keywords-performance evaluation; attack mechanisms; performance metrics; MANET security

I. INTRODUCTION

As mobile ad hoc networks (MANETs) are created spontaneously with mobile nodes that continuously change locations they are particularly susceptible to attack. Several attack mechanisms have been proposed and partially corresponding detection and counter measures. However, the majority of these approaches have been analyzed and evaluated with incongruent objectives, varying setups and performance metrics. Simulation results are thus not commensurate due to application-specific parameter sets and implementation differences. The objective of our analysis is to implement and evaluate the most prominent attacks using a consistent and comparative methodology. The overall impact of each attack is captured and thoroughly analyzed

based on a suitable set of performance metrics. We define requirements for thorough and consistent capturing of the effects of all considered attack types. A comprehensive list of metrics is selected accordingly and used for the analysis using various combinations of attack types and parameter sets.

We examine possible strategies of attacking nodes to maximize their impact while minimizing their risk of detection, and show the impact of the investigated attacks on the network performance. Using our results attackers are able to choose a setup with lowest detection probability and MANET operators are able to estimate damage levels of a specific attack type and determine adequate counter measures.

Performance metrics defined in this paper enable a consistent comparison of a range of attack types with various parameters sets which can provide deeper insight into the interaction and impact of attacking nodes on MANETs. Our evaluation results show that the degree of impact of attacks differs significantly depending on attack type and parameters used. The impact of certain types of attacks increases if a larger number of attackers are present whereas particular attack types (e.g. flooding and route disruption attacks) are most efficient when a single attacker is present.

The remainder of this paper is structured as follows: Section II provides a brief review of related work followed by the problem definition. Standard attacks on MANETs and performance metric requirements capturing the effects of each attack type are outlined in Section III. In Section IV the selection and definition of suitable performance metrics are presented and subsequently used in Section V to describe observed results in evaluation experiments. Conclusions and an outlook on future research opportunities finalize the paper in Section VI.

II. RELATED WORK

Several attacks have been proposed for use in MANET environments as well as protocols that detect and defend against them. Two of the more prominent attacks described in MANET routing literature are wormhole attacks and black

hole attacks. A wormhole attack [1] uses two cooperating corrupted nodes of a network connected by an out-of-band channel to re-route data traffic. The black hole attack [2], [3] by contrast is based on the concept of generating and transmitting incorrect route information to attract traffic. Data packets are thus not forwarded to the proper recipient node but are instead “sucked in” by the attacking node, similar to a black hole.

Packet dropping (among other attacks) is addressed by Marti *et al.* who proposes a mechanism called watchdog [4] that identifies misbehaving nodes. Another module called pathrater helps routing protocols to bypass these misbehaving nodes. Balakrishnan *et al.* propose in [5] a mechanism to defend against flooding and packet drop attacks in MANETs. They present an obligation-based model called fellowship and describe how this model can be used to identify and penalize malicious and selfish nodes.

Bo *et al.* [6] present a performance comparison of different routing protocols under attack. They compare three different routing protocols under attack by two types of selfish nodes: Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR), and Ad hoc On-Demand Distance Vector (AODV). Evaluation metrics are average packet delay, normalized throughput, routing overhead and routing load. Their evaluation results show that DSDV is the most robust routing protocol under the considered attacks.

Juwad and Al-Raweshidy present in [7] an experimental performance comparison between Secure-AODV (SAODV) and AODV. They claim that there has been a lack of performance and security analysis in real network test-beds. A quantitative performance comparison between routing protocols AODV and SAODV is presented in an experimental test-bed and using the OPNET network simulator. These results show that SAODV is more effective in preventing two types of attacks (control message tampering and data dropping attacks) than AODV. Chen *et al.* quantitatively evaluate an approach detailing network survivability in wireless ad hoc networks [8]. They define network survivability as a combination of network failure impacts and failure durations and use a performance metric called excess packet loss due to failures.

III. PROBLEM DEFINITION

In this section we describe typical MANET attacks and outline requirements that performance metrics which are suitable for impact measurements should satisfy.

A. Attacks on MANETs

For each attack we give a general introduction and outline how it can be implemented using the AODV [9] protocol, which is the basis for the evaluation performed in this paper.

Attacks on MANETs can be categorized in several ways. One method of characterization is to distinguish them according to their objective: Denial-of-Service (DoS) attacks

for example try to disturb normal network and/or node operation while others attempt to completely terminate all activity (e.g. black hole and flooding attacks). Still other attack mechanisms aim to garner a more powerful position in the network by manipulating routing packets (e.g. wormhole attacks) which allows attackers to eavesdrop and manipulate packets (e.g. to break confidentiality and integrity).

1) *Black Hole Attack:* The black hole attack [2], [3] generates and disseminates incorrect routing information so that packets are no longer forwarded to the intended recipient; instead they are lost or forwarded to an attacking node. Fig. 1 shows an example of normal data traffic transferred via adjacent nodes to node *D* on the left and the effects of a successful attack on the right. Messages intended for node *D* do not reach their desired target but are instead intercepted by the attacking node.

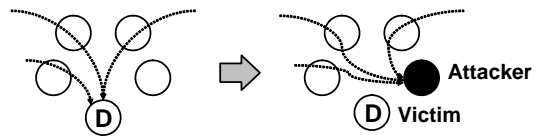


Figure 1: Data flow to target *D* before and during a black hole attack

In an implementation using AODV an attacker may distribute manipulated Route Reply (RREP) messages in order to be included in many valid network routes and to appear as an attractive relay for as many target nodes as possible. When the attacker receives a Route Request (RREQ) message it creates and sends a manipulated RREP message indicating a shorter transport distance through that node. Attackers also have the option of manipulating only a fraction of RREP messages to reduce probability of detection. Hop counts of manipulated RREP messages are decreased in order to purport to have shorter routes to the destination node. Sequence numbers are also increased to make messages appear newer and thus increase the probability that the sending node will accept them.

2) *Flooding Attack:* Flooding attacks have the dangerous characteristic that they are simple to implement but may cause high damage. An attacker can create and send messages with varying destination addresses, varying content and varying time-to-live (TTL) values into the MANET. The goal is to increase network load and thus the load of each network participant. Network nodes are therefore occupied with packet forwarding and have less time to perform other tasks. Target nodes may be randomly selected from nodes listed in the routing table of the attacking node. Messages are generated with a maximum TTL value sent to the chosen target nodes to flood the network with messages.

3) *Packet Dropping Attack:* A packet dropping attacker discards all or a fraction of received messages. One option for AODV is to drop only specific types of routing messages

– RREQ, RREP, or Route Error (RERR) – or in general all routing messages. Alternatively attackers may also discard all or a percentage of messages, the latter having the advantage to be more difficult to detect as there is no permanent influence on the network.

4) *Route Disruption Attack*: This type of attack attempts to disrupt MANET routing processes by sending manipulated routing messages that include source and/or destination nodes that do not exist in the MANET. Distribution of routing messages referring to non-existent nodes not only increases network load but nodes may also add non-existent routes to their routing tables.

Two variants of this attack are possible in AODV: one sending RREQ messages with a fake target node, the other sending RREP messages with forged sender node. The first step to achieve a successful attack using this method is to create a node ID not yet listed in the routing table of the attacker (which does however not guarantee that such a node does not exist in the network). In the first variant the attacker generates a RREQ message with a created node ID as target node and sends it with a TTL value set to maximum. In the second variant the attacker generates a RREP message with an existing node as destination but with a fake ID as sender ID. Additionally sequence numbers of messages are incremented before they are sent.

5) *Wormhole Attack*: Wormhole attacks [1] use two cooperating network nodes to re-route data traffic. In order for this to be successful the two nodes must “ally” themselves and establish an additional channel outside normal network communications serving as a tunnel. Wormhole attacks are named as such as they mimic this hypothetical physical phenomenon. In this type of attack the two nodes mask that they are not directly adjacent nodes, instead they pretend to be neighbors and therefore dispose fast connections to each other and their neighbors. As these paths are used for sending data that is not part of the proper network wormholes are very difficult to detect.

Wormholes themselves are not necessarily only negative for a network as such a shortcut can have positive benefits such as relief for network traffic or shorter transfer times for packets on routes containing the wormhole. Attackers use wormholes in the network to make their nodes appear more attractive (with perceived faster transfer times) so that more data is routed through their nodes.

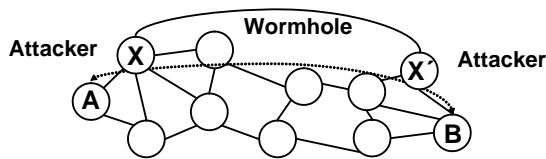


Figure 2: Data flow during a wormhole attack of X and X'

An example is shown in Fig.2. An attacker X receives

a RREQ message for a destination node B . The target is located in the vicinity of the second attacker X' . X sends the RREQ message via the external connection to X' who forwards it on to B . Due to the fast external connection an RREP message forwarded in this way reaches B faster and with a lower hop count than messages that travel on a regular, internal path. B therefore selects the route that belongs to the RREQ message that was forwarded by the attacking nodes and sends a RREP message back to A via this route. Attackers attract and redirect a significant portion of network traffic in this way, giving them a stronger position in the network.

B. Requirements for Suitable Performance Metrics

In this section we outline requirements for performance metrics that thoroughly capture the effects of particular attacks on MANETs. In general these requirements should represent relevant properties of MANETs and illustrate changes that are caused by a specific attack type [10]. They should also provide sufficient data to allow a detailed analysis of each effect, for example it is expected that during a flooding attack network load increases so there should be at least one metric that captures this effect.

We define the following criteria for these purposes. The first criterion is that metrics should be applicable for MANETs. As MANETs have differing properties to other network types (e.g. wired networks) metrics are selected that measure performance values or conditions that are present in MANETs and that are measurable.

Attacks can generally be categorized in two classes which correspond to the following criteria. Suitable metrics should therefore satisfy at least one of the following two criteria in order to be considered for the evaluation.

- *Detection of Denial-of-Service Attacks* Most attacks try to affect network performance in order to implement a DoS attack. They may disturb or disrupt the basic network functionality or completely deactivate it for longer periods of time (cf. Section III-A), therefore it is important to have metrics that measure the impact of an attack on the level of service that is provided by the network on each layer. Furthermore detection of increased network load or overload is also an important metric that provides overall effect perspective. This criterion applies for DoS attacks such as black hole, route disruption, flooding and packet dropping.
- *Detection of Routing and Network Topology Manipulation* Another class of attacks attempt to change routing and network topology in order to be included in as many routes as possible thus increasing access to transmitted packets. In this way attacking nodes gain a more powerful position in the network (cf. Section III-A). Metrics are therefore required that capture the influence of attacks on routing behavior and network

topology. This criterion applies for attacks that manipulate routing behavior such as black hole and wormhole attacks.

IV. PERFORMANCE METRICS

In this section we select suitable performance metrics according to each requirement defined in the above section. We describe how each metric covers certain relevant aspects for the analysis and then specify how they are calculated.

Metric	Denial of Service (DoS)	Routing and Network Topology Manipulation
Application Layer Achievable Bandwidth (AppLAB)	✓	X
One-Way Delay (OWD)	✓	✓
Round Trip Delay (RTD)	✓	✓
Delay Variance (DV)	✓	X
Queue Length (QL)	✓	X
Packet Delivery Ratio (PDR)	✓	X
Packet Loss Ratio (PLR)	✓	X
Path Optimality (PO)	✓	✓
Routing Overhead (RO)	✓	X
Route Length per Packet (RLpP)	X	✓

Table I: Criteria for suitable performance metrics are indicated by columns DoS and Routing and Network Topology Manipulation, “✓” indicates that the criterion is met, “X” that it is not met.

Based on requirements defined in the previous section we select suitable metrics that cover all relevant aspects regarding each attack variant. Table I shows an overview of considered metrics and requirements that they meet. Application Layer Achievable Bandwidth (AppLAB) measures what level of service is provided to the application layer (to the user). This metric is therefore the most important metric for overall MANET performance. One-Way Delay (OWD), Round Trip Delay (RTD) and Delay Variance (DV) describe the properties of delay times which are important for certain applications, e.g. real time applications such as voice-over-IP. We select OWD to capture this aspect. For wormhole attacks it is expected that due to the additional out-of-band connection OWD values may decrease affected connections.

Queue Length (QL), Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR) are related to the amount of packets that do not arrive to the intended target. Routing Overhead (RO) describes the overhead introduced by a specific attack which may lead to denial of service. These are important measures for DoS attacks. We select PLR as representative for this category. Path Optimality (PO) and Route Length per Packet (RLpP) detect topology manipulations and changes in routing behavior. We select RLpP to capture these effects. Changes in network topology (e.g. caused by wormhole attacks) may provide shorter routes and therefore a decrease in RLpP values.

The specification of the selected metrics is described in detail in Table II.

Name	Application Layer Achievable Bandwidth (AppLAB)
Unit	$\frac{Bit}{s}$
Layer	Application layer
$\varnothing_{AppLAB} = \frac{\sum \text{amount of received data (data packets)}}{\text{simulation duration}}$	
Name	One-Way Delay (OWD)
Unit	Seconds
Layer	Application layer
$\varnothing_{OWD} = \frac{\sum \text{one way delay of each received data packet}}{\sum \text{received data packets}}$	
Name	Packet Loss Ratio (PLR)
Unit	Percentage
Layer	Application layer
$\varnothing_{PLR} = \frac{\sum \text{dropped data packets}}{\sum \text{sent data packets}}$	
Remark	Dropped data packets contains all packets that had to be dropped because of mobility or full queues or by attackers.
Name	Routing Overhead (RO)
Unit	Percentage
Layer	Network layer
$\varnothing_{RO} = \frac{\sum \text{sent, received and forwarded routing packets}}{\sum \text{sent, received and forwarded routing and data packets}}$	
Name	Route Length per Packet (RLpP)
Unit	Hops
Layer	Network layer, Application layer
$\varnothing_{RLpP} = \frac{\sum \text{route length of each received data packet}}{\sum \text{received data packets}}$	

Table II: Specification and description of the performance metrics used

V. PERFORMANCE EVALUATION

In this section we present the evaluation results for each attack using the metrics defined above. We analyze the results and summarize important aspects. We then discuss and compare the influence of attack type and parameter settings on the impact caused by an attack and derive particular conclusion about effectiveness and suspiciousness of specific attacks.

A. Simulation Environment and Parameters

For evaluation purposes the JiST/MobNet [11] network simulator has been extended with attack mechanisms as outlined in Section III-A. Several simulations were performed in MANET scenarios using AODV as routing protocol.

36 nodes are placed on a simulation field 900m by 900m. Radio range is set to 250m and a random way point mobility model is used with zero pause time and a speed between one and two meters per second. Five parallel data streams

Type of Attack	Parameters	Values
Black Hole	Data packet drop rate	100%
	Attack propability	75%, 87.5%, 100%
Flooding	Data packet drop rate	0%
	On-time	100s
	Off-time	0s, 25s
Packet Dropping	Number of destinations	5, 7, 10
	Data packet drop rate	0%, 100%
	Routing packet drop rate	0%, 75%, 100%
Route Disruption	Packet types	RERR, RREP, all
	Data packet drop rate	0%
	On-time	100s
Wormhole	Off-time	0s, 25s
	Packet types	RREQ, RREP
	Data packet drop rate	100%
	Number of attackers	2, 4, 6

Table III: Attack specific parameter sets for evaluation series

between randomly chosen nodes are created with constant bit rate (1024 bytes per second, 512 bytes per packet). These data streams randomly change every 30 seconds. One to five of the nodes are configured as attacking nodes with attack types and parameters sets shown in Table III. Three hundred simulation runs were performed for each parameter set.

For each attack several runs of parameters have been performed to optimize parameters and find the most effective parameter combinations. Parameters chosen for evaluation within this paper are a result of this optimization process.

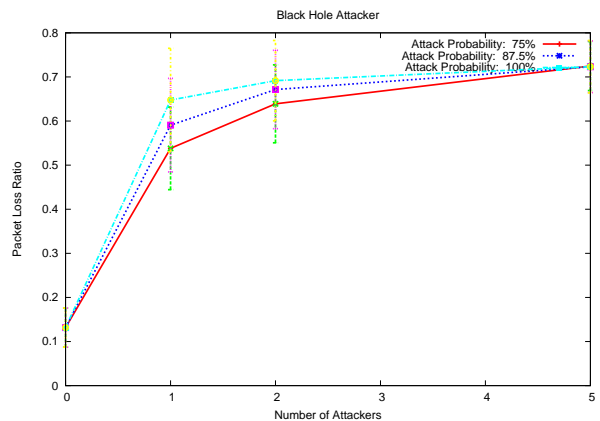
B. Results

Simulation results are outlined below and summarized to highlight important aspects for each attack. We then discuss and compare the influence of parameter settings on the impact caused by an attack and derive particular conclusion about effectiveness and suspiciousness of each specific attack.

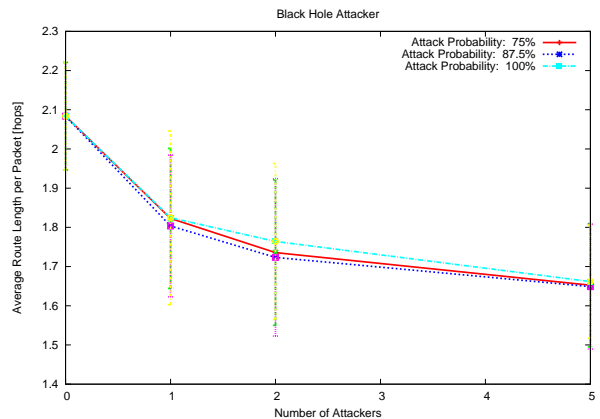
For brevity sake we choose the most illustrative metrics for each attack type and present related results in diagrams. Each diagram includes mean values for each measurement value and the standard deviation indicated by a vertical bar.

The results for AppLAB are described afterwards in a common section for all attack types. This metric is the most important metric as it indicates the quality of the communication service that is provided to the user and therefore allows a comparison of the overall impact of all attack type.

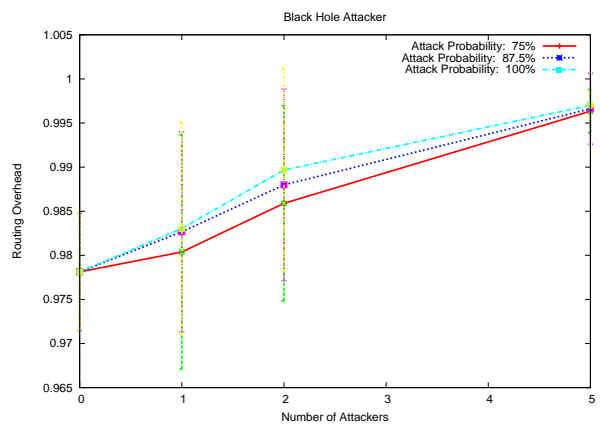
1) *Black Hole Attack*: Results for black hole attacks are shown in Fig. 3. This attack type redirects all packets in its vicinity to itself using fake RREP messages and drops packets that it receives with a specific probability. This strategy generally has the biggest impact on the MANET compared to the other attacks. PLR (cf. Fig. 3a) shows an increase when only a single attacker is present from 0.13 (without an attacker) to more than 0.5 for all parameter settings (i.e. at least four times as high). The increase is



(a) Packet Loss Ratio (PLR)



(b) Route Length per Packet (RLpP)



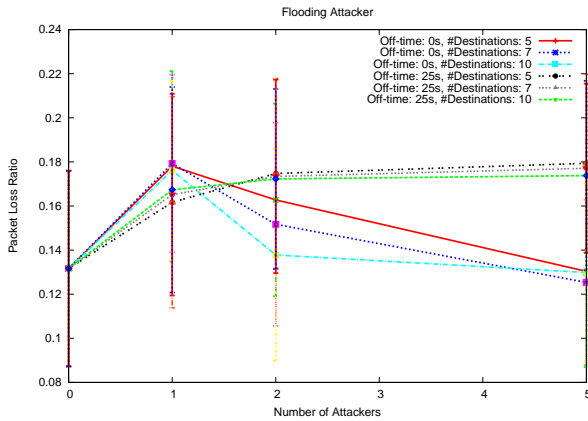
(c) Routing Overhead (RO)

Figure 3: Results for black hole attack – *Fixed parameters*: Data packet drop rate = 100% – *Variable parameters*: Attack probability = 75%, 87.5%, 100%

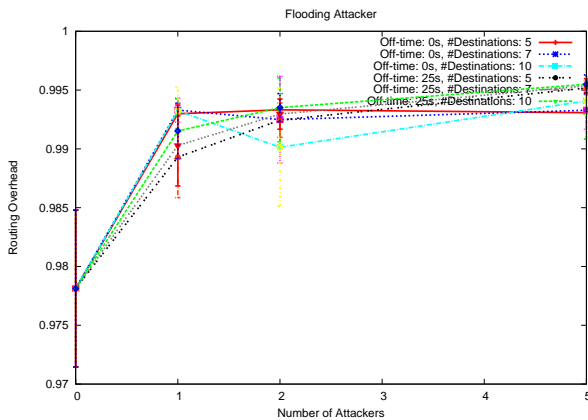
however not as significant for 2 and 5 attackers. RLpP (cf. Fig. 3b) decreases monotonously with the number of

attackers as black hole attackers provide seemingly very short routes.

RO (cf. Fig. 3c) increases monotonously with the number of attackers due to two factors: black hole attackers decrease the number of data packets that are successfully forwarded in the network and additional routing messages are created and transmitted by the attacker. This attack achieves highest impact levels with the largest number of attackers and the lowest AppLAB values for all attack types.



(a) Packet Loss Ratio (PLR)



(b) Routing Overhead (RO)

Figure 4: Results for flooding attack – *Fixed parameters*: Data packet drop rate = 0%; On-time = 100s – *Variable parameters*: Off-time (pause) = 0s, 25s; Number of Destinations = 5, 7, 10

2) *Flooding Attack*: Results for flooding attacks are shown in Fig. 4. A notable property for this attack type is that only one attacker is required for an effective attack. Additional attackers do not increase overall impact levels and should therefore implement other attack types to increase effectiveness. The most effective setup is one attacker with 100 seconds on-time and 25 seconds off-time, the number of recipients is not as relevant. This set causes the highest

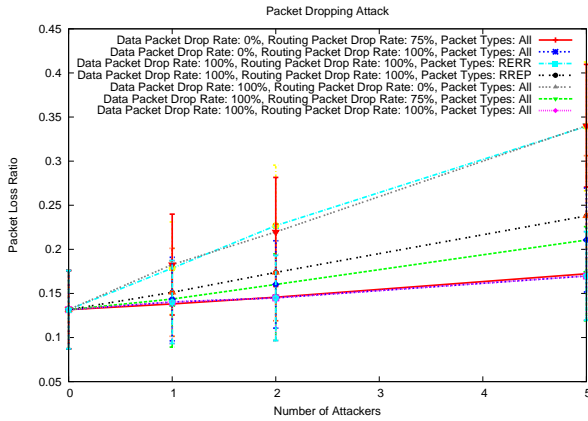
aggregate amount of damage to the MANET but also garners the least amount of suspicion of all setups tested. PLR (cf. Fig. 4a) increases significantly when an attacker is present. Additional attackers however increase overall impact only slightly. The attacker should be permanently active to be effective.

A remarkable observation is that PLR decreases for two or more attackers when the attackers are permanently active. The results for RO (Fig. 4b) may explain why this happens. RO decreases (at least for scenarios without pause time) with more than one attacker: active attackers send many RREQs, therefore nodes get to know many valid routes in the network and do not need to newly request and establish them. Some additional optimization experiments were performed with other parameter sets, they did not however provide any significant improvement. The highest damage levels regarding AppLAB for this attack is a reduction of approximately six percent.

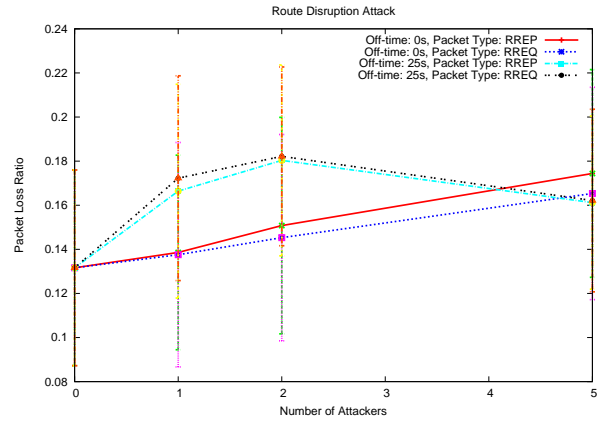
3) *Packet Dropping Attack*: Results for packet dropping attacks are shown in Fig. 5. This attack type drops routing packets and optionally data packets (similar to black hole attack). Setups that drop data and routing packets as well as attackers that only drop routing packets were evaluated in order to compare results with other attack types: setups with data packet dropping for comparison with black hole attacks, setups without dropping of data packets for flooding and route disruption attacks. Test results show that dropping of routing packets does not increase the impact of an attack as this contradicts the goal of dropping data packets: If an attacker drops all received routing messages, no routes can be established via this node, consequently no data packets are sent via the attacking node and the attacker cannot drop data packets.

PLR (cf. Fig. 5a) has the largest impact for 100% drop rate of RERR messages, results for the same parameter set without dropping of routing messages are however almost identical. For all attacks that do not drop data packets RREP dropping delivers the largest PLR values and is therefore a preferable setup for an attacker. RO (cf. Fig. 5b) increases when attackers are present as they drop all routing messages and therefore normal nodes have to resend RREQ messages. This also affects queue length and leads to increased PLR. Impact of attack increases as the number of attackers increases for all attacks. Most damage regarding AppLAB is therefore achieved with the largest number of attackers who drop data and RERR packets; damage is however still three times lower than for black hole attacks.

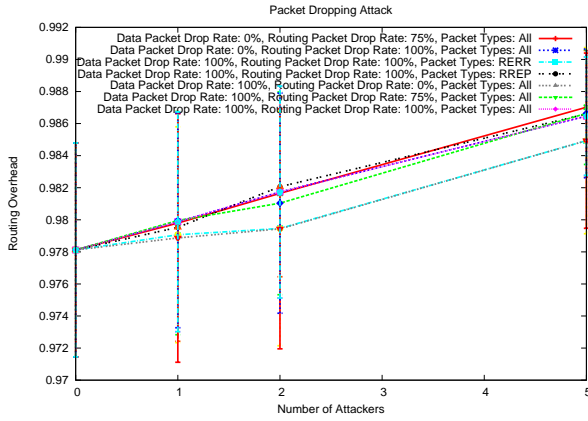
4) *Route Disruption Attack*: Results for route disruption attacks (cf. Fig. 6) show that only two attackers should be used for this type of attack; additional resources can be utilized elsewhere as they do not increase performance of the attack if used for the initial disruption attack. The type of routing messages that are forged has a minor effect on performance, RREQ messages are however slightly



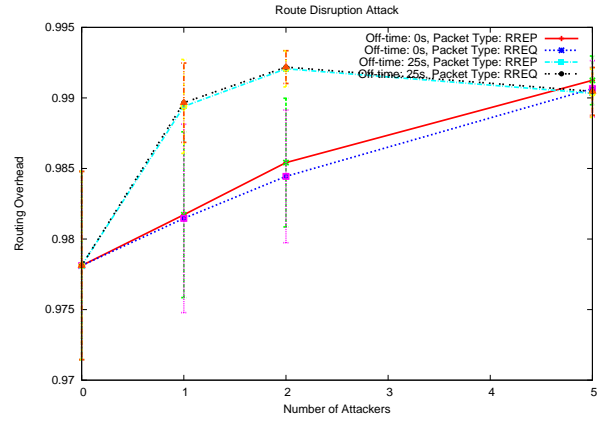
(a) Packet Loss Ratio (PLR)



(a) Packet Loss Ratio (PLR)



(b) Routing Overhead (RO)



(b) Routing Overhead (RO)

Figure 5: Results for packet dropping attack – *Variable parameters*: Data packet drop rate = 0%, 100%; Routing packet drop rate = 0%, 75%, 100%; Packet types to be dropped = RERR, RREP, all

Figure 6: Results for route disruption attack – *Fixed parameters*: Data packet drop rate = 0%; On-time = 100s – *Variable parameters*: Off-time (pause) = 0s, 25s; Type of routing message: = RREQ, RREP

preferable over RREP messages. PLR values (cf. Fig. 6a) are higher for attackers with an off-time of 25 seconds than for attackers without off-time; this effect increases for two attackers but starts to diminish with five attacking nodes.

The effects of this attack are similar to those of flooding attacks. Attackers with no off-time send several times as many routing messages as attackers with pause time, but RO (cf. Fig. 6b) is higher with pause time. This effect might be explained by the increased PLR values: when the amount of successfully transmitted data packets decreases, the routing overhead increases. Lowest AppLAB values for this attack are achieved with two attackers. The largest impact on AppLAB observed was a decrease of approximately six percent (similar to flooding attacks).

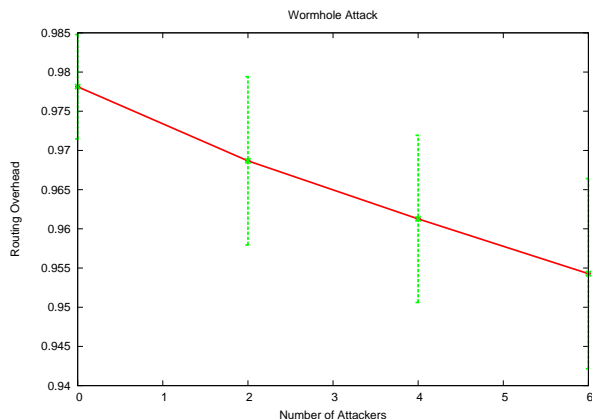
5) *Wormhole Attack*: Results for wormhole attacks are shown in Fig. 7. It is difficult to completely capture the impact of this attack as it does not disrupt network operation

but instead reshapes network topology and redirects traffic. Changes in MANET performance metrics can indicate the effectiveness of this type of attack.

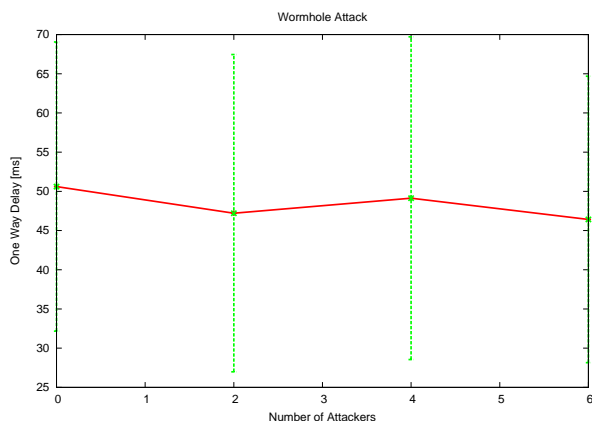
Reduced RO values (cf. Fig. 7a) indicate that routing messages are forwarded on the out-of-band connection and that more efficient routes can be found. Consequently PLR values also slightly decrease. RLpP and OWD (cf. Fig. 7b) do not as expected significantly decrease. This might be due to the small simulation area of 900 by 900 meters used with respect to the radio range of 250 meters. The out-of-band channel provided by Wormhole attacks may be more attractive in larger simulation areas and consequently more effective.

C. Summary

Our results show that the impact of certain types of attacks increases if additional attacking nodes are present. Particular



(a) Routing Overhead (RO)



(b) One-Way Delay (OWD)

Figure 7: Results for wormhole attack – *Fixed parameters:* Data packet drop rate = 0%; On-time = 100s; Off-time (pause) = 0s – *Variable parameters:* Number of Attackers: 2, 4, 6

attack types (flooding and route disruption) already achieve (more or less) their highest level of effectiveness when a single attacker is present. These results can be used by an attacker to choose a less suspicious strategy with a similar impact to counter detection.

Table IV shows an AppLAB overview of all attacks for various numbers of attackers. This represents the most important metric as it indicates the quality of the communication service that is provided to the application and therefore to the user of the network. Black hole attacks generally have the largest impact on MANET performance; they decrease AppLAB up to 31 %. Packet dropping (routing and data packets) has the second highest impact with up to 24 %. Flooding, packet dropping (only routing messages) and route disruption attacks are similarly effective with an AppLAB reduction of around 5 % to 6 %. On the contrary

Wormhole attacks increase AppLAB performance as they provide an additional out-of-band connection that can be used by other network nodes.

Attack Type	Number of Attackers			
	0	1	2	5
Black Hole	100%	40,32%	35,14%	31,29%
Flooding	100%	93,96%	94,05%	94,44%
Packet Dropping	100%	94,59%	89,04%	76,06%
Packet Dropping (only routing messages)	100%	96,05%	95,47%	94,06%
Route Disruption Attack	100%	95,03%	94,13%	95,04%
Wormhole	100%	101,69%	101,32%	100,99%

Table IV: Overview of damage caused by different attack types according to Application Layer Achievable Bandwidth (AppLAB)

VI. CONCLUSION AND OUTLOOK

In this paper we implemented and evaluated the most prominent attacks in a consistent manner to provide a concise comparison of attack types and parameters. We defined performance metrics that allow the capture and analysis of impact levels for each attack type on MANET performance. An exploration of the influences and damage levels caused by several attack types and parameter sets has also been presented.

Our evaluation results show that the degree of impact for each attack type differs significantly depending upon parameters used. The impact of particular attacks increases considerably with an increasing number of attacking nodes in several of the scenarios, whereas other attack impact levels remain almost constant with varying number of attackers. These results imply that an attacker could choose an attack strategy from a number of alternatives with similar overall impact which minimizes detection risk. This also suggests that MANET operators can use the results to estimate damage caused by various attacks to determine adequate counter measures.

Performance metrics outlined in this paper provide a basis for consistent comparison of various attack types and parameters and thus a deeper insight into the interaction and the impact of attacks in MANETs. The influence of varying simulation setups (e.g. regarding simulation area and node mobility) however should be further investigated in future work. Using this framework future research on attacks in MANETs can focus on the most fraudulent attacks and investigate and compare in more detail their specific properties.

REFERENCES

- [1] W. Wang and B. Bhargava, “Visualization of Wormholes in Sensor Networks,” in *Proceedings of the 2004 ACM Workshop*

on *Wireless Security*. Philadelphia, PA, USA: ACM Press, Oct. 2004, pp. 51–60.

- [2] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Denial of Service Resilience in Ad Hoc Networks,” in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking*. Philadelphia, PA, USA: ACM Press, Sep. 2004, pp. 202–215.
- [3] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” in *Proceedings of the 42nd Annual ACM Southeast Regional Conference*. Huntsville, AL, USA: ACM Press, Apr. 2004, pp. 96–97.
- [4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” in *Proceedings of the 6th Annual International Conference on Mobile computing and Networking*. Boston, MA, USA: ACM Press, Aug. 2000, pp. 255–265.
- [5] V. Balakrishnan, V. Varadharajan, and U. Tupakula, “Fellowship: Defense against Flooding and Packet Drop Attacks in MANET,” in *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, April 2006, pp. 1–4.
- [6] S. M. Bo, H. Xiao, A. Adereti, J. A. Malcolm, and B. Christianson, “A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack,” in *IAS '07: Proceedings of the Third International Symposium on Information Assurance and Security*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 50–55.
- [7] M. Juwad and H. S. Al-Raweshidy, “Experimental Performance Comparisons between SAODV & AODV,” in *AMS '08: Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 247–252.
- [8] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, “Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks,” *Wireless Networks*, vol. 8, no. 5, pp. 481–494, 2002.
- [9] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” Internet Engineering Task Force, Request for Comments 3561, July 2003. [Online]. Available: <http://www.ietf.org/rfc/rfc3561.txt>
- [10] P. Ebinger and M. Parsons, “Measuring the Impact of Attacks on the Performance of Mobile Ad hoc Networks,” in *ACM PE-WASUN: Proceedings of the 6th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, Tenerife, Canary Islands, Spain, 2009.
- [11] T. Krop, M. Bredel, M. Hollick, and R. Steinmetz, “JiST/MobNet: Combined Simulation, Emulation, and Real-world Testbed for Ad hoc Networks,” in *WiNTECH 07*. ACM, September 2007.