# TOGBAD-LQ - Using Challenge-Response to Detect Fake Link Qualities

Elmar Gerhards-Padilla, Nils Aschenbruck, and Peter Martini

University of Bonn - Institute of Computer Science 4
Römerstr. 164, 53117 Bonn, Germany
{padilla, aschenbruck, martini}@cs.uni-bonn.de

## Abstract

The usage of link quality based routing metrics significantly improves the quality of the chosen paths and by that the performance of the network. But, attackers may try to exploit link qualities for their purposes. Especially in tactical multi-hop networks, routing may fall prey to an attacker. Such routing attacks are a serious threat to communication. TOGBAD is a centralised approach, using topology graphs to detect routing attacks. In this paper, we enhance TOGBAD with the capability to detect fake link qualities. We use a Challenge/Response method to estimate the link qualities in the network. Based on this, we perform plausibility checks for the link qualities propagated by the nodes in the network. Furthermore, we study the impact of attackers propagating fake link qualities and present simulation results showing TOGBAD's detection rate.

Digital Object Identifier 10.4230/OASIcs.KiVS.2011.85

## 1 Introduction

In tactical environments (i.e. military or disaster response scenarios) sensitive data (e.g. soldier positions) is transmitted via insecure links. In addition, there is a high probability of hostile units and the disturbance or eavesdropping of communication may lead to severe consequences, in the worst case even to loss of human life. Thus, secure communication is mandatory in tactical environments.

To enable secure communication, as a first step it is necessary to reliably enable communication. The performance of a network depends on the routing protocol used. Furthermore, the routing protocol's performance heavily depends on the routing metric used. Link quality based metrics have been shown to outperform simple routing metrics like minimum hop-count (e.g. [5, 20, 8]). These metrics should be used to provide high quality routes in the network and by that reliable communication. While it is undoubtedly reasonable to use link quality based routing metrics, it also opens an additional point of attack. An attacker may try to disturb network operation or eavesdrop traffic by propagating fake link qualities.

As mentioned, there is a high demand for security in tactical multi-hop networks. Fortunately, these networks possess a property that can be exploited for security purposes. In such scenarios, there typically exists a command and control structure. The communication necessary for this structure leads to two types of nodes: fully equipped and light-weight nodes. The fully equipped nodes have access to power supply and therefore use more powerful hardware. The light-weight nodes use battery-driven and therefore not so powerful devices. As an example one may think of a hostage rescue scenario, where the fully equipped node is an armoured vehicle, while the light-weight nodes are infantry units. We assume that key material is installed in advance of the tactical mission. Thus, all key material necessary is available at the nodes.

In the following, we consider insider attacks, i.e. attacks of nodes owning valid keys. For example, these attacks may be performed by attackers taking over nodes owning valid keys.

17th GI/ITG Conference on Communication in Distributed Systems (KiVS'11).
Editors: Norbert Luttenberger, Hagen Peters; pp. 85–96
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

One way to detect such attacks is to use intrusion detection, or to be more specific anomaly detection. TOGBAD [7, 6], is an anomaly detection approach using topology graphs to counter routing attacks in tactical multi-hop networks. It exploits the structure of tactical multi-hop networks by running the detection instances on the fully equipped nodes.

In its basic version TOGBAD is not able to deal with fake link qualities. Nevertheless, with its detection and communication infrastructure it provides a very good basis for detecting fake link qualities. Thus in this paper, we enhance TOGBAD with fake link quality detection capability. In detail, we use a Challenge/Response method to locally estimate the link qualities in the network. Based on this, we locally perform plausibility checks for the link qualities propagated in each node's neighborhood, send important observations to a central instance and centrally decide whether there is an attack. Furthermore, we present studies on attackers sending fake link qualities and an evaluation of TOGBAD's detection.

The remainder of this paper is structured as follows. We first introduce routing attacks (Sect. 2). Afterwards, we present related work in the field of detection and prevention of routing attacks in multi-hop networks taking into account fake link qualities (Sect. 3). The following section introduces TOGBAD, our approach to detect routing attacks and our recent enhancements to it (Sect. 4). After that, we first introduce our simulation environment (Sect. 5.1) and then show our evaluation concerning the quality of TOGBAD-LQ (Sect. 5.2). Finally, we conclude the paper (Sect. 6).

## 2 Routing Attacks

In wireless multi-hop networks (e.g. Mobile Ad Hoc Networks (MANETs), Mesh networks), every node of the network may be part of the routing process. Hence, it is quite easy for a node to influence routing in such networks. An attacker sending false routing information can try to attract routes and by doing so gain access to data transmitted in the network. Having gained this access, an attacker may try to achieve different goals: eavesdrop, manipulate or drop traffic. This kind of attacks is already mentioned in [12], [10],[11], and [13]. In this paper, we focus on an attack known as sinkhole attack.

### 2.1 Sinkhole Attack

The terms black hole, gray hole, and sinkhole attack are used for quite similar attacks. The approach of the attacker is the same for all three attacks. The attacker propagates fake routing information and by that attracts routes. The differences between the three attacks are the attacker's actions after having attracted routes. In a black hole attack, the attacker drops all traffic of the attracted routes. In a gray hole attack, the attacker selectively drops traffic and in a sinkhole attack selectively drops or manipulates traffic. In this work, we consider and detect an attacker propagating fake link qualities. The attacker does this to attract routes. Thus, we detect the basis for all three attacks and for our purpose it is not of interest whether the attacker tries to create a black hole, wormhole or sinkhole. Since the sinkhole attack is the most general one, we will use the term sinkhole attack in the following.

The actual implementation of a sinkhole attack strongly depends on the routing protocol and routing metric used in the network. Many protocols, such as Optimized Link State Routing (OLSR) [4], OLSRv2 [3] and Simplified Multicast Forwarding (SMF) [16], use so called HELLO messages to discover their neighborhood and link qualities. These messages are a good starting point for an attacker to propagate fake link qualities and, by doing so, gain a privileged position in the network.

## 2.2 Neighborhood Discovery Protocol

The use of HELLO messages to determine a node's neighborhood is standardized in the Neighborhood Discovery Protocol (NHDP) [2]. According to this draft, each node periodically spreads HELLO messages announcing its neighborhood. By these messages, each node learns about its 1-hop and 2-hop neighborhood. In this draft, link quality is only used locally to guarantee a minimum quality of links. The link qualities are not used in signaling nor in a link metric. The neighborhood discovery standardized in the Neighborhood Discovery Protocol is used by a variety of routing protocols like OLSR [4], OLSRv2 [3] or SMF [16]. However, in none of these protocols a link quality based routing metric is integrated, although it has been shown, that link quality based routing metrics lead to significantly improved network performance (cf. [5, 20]).

## 2.3 Expected Transmission Count

One link quality based routing metric is the Expected Transmission Count (ETX) [5]. Its idea is to minimize the number of packet transmissions required to successfully deliver a packet. It measures two kinds of link qualities to calculate the ETX-value: (1) link quality and (2) neighbor link quality.

The link quality (LQ) depicts the quality of the link in direction from the neighbor node to the node signaling the link quality. Hence, it is measured by the node itself. The neighbor link quality (NLQ) depicts the quality of the link in direction from the node to the neighbor node. Therefore, it is measured by the neighbor node. A correctly behaving node, takes the last link quality signaled by the neighbor as next neighbor link quality for the link to the neighbor. From link quality and neighbor link quality the ETX-value is calculated in the following way: $ETX = \frac{1}{LQ*NLQ}$

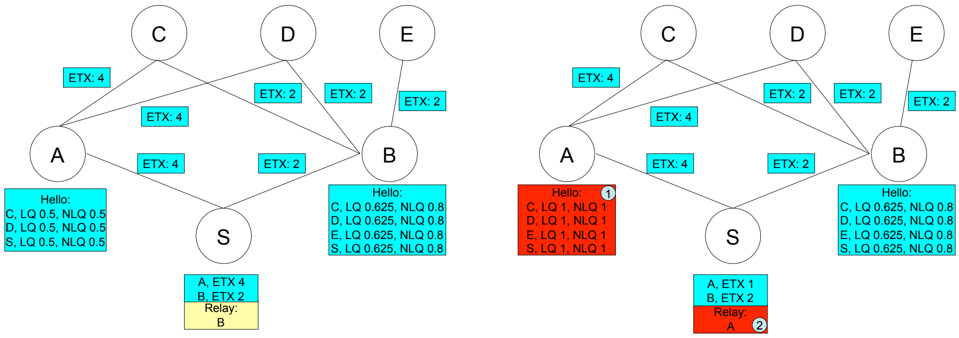
To clarify the signaling of link qualities, we consider a small example. Consider a link between nodes A and B. In the direction A→B 80% of the packets reach node B. In the opposite direction B→A 70% of the packets reach node A. Node A would signal a link quality of 70% and a neighbor link quality of 80%. Node A would know about the neighbor link quality value from node B's last HELLO message. In this message node B would have signaled a link quality value of 80%.

The ETX metric has been shown to significantly increase the network performance in testbeds (cf. [5]) and performs very well under real world conditions (e.g. in various Freifunk networks in combination with OLSR as routing protocol). Thus, in the following we use SMF with NHDP and ETX for routing purposes. To enable the use of ETX together with NHDP, link qualities have to be signaled. Thus, link qualities are added to the HELLO messages. Each node includes for each of its links a link quality and a neighbor link quality value in its HELLO messages.

## 2.4 Sinkhole in SMF with NHDP and ETX

SMF is a multicast forwarding approach suitable for multi-hop networks. Its basic idea is to forward multicast data using efficient flooding via a selected set of nodes, the relay set. SMF needs three logical components: Neighborhood Discovery Protocol, Relay Set Selection Algorithm, and Forwarding Process.

The Neighborhood Discovery Protocol specifies how nodes determine their neighborhood. Based on this neighbor information, the Relay Set Selection Algorithm chooses the set of relay nodes. On the basis of neighbor information and relay set selection, the forwarding process decides whether an incoming packet is forwarded by the receiving node.



**(a)** SMF without Sinkhole

**(b)** SMF with Sinkhole

**Figure 1** Example for SMF

In this paper, we focus on SMF using NHDP (cf. Section 2.2) and ETX (cf. Section 2.3). The neighborhood discovery is done according to NHDP. The relay set selection takes into account link qualities. The neighbor with the highest link quality and reaching at least one 2-hop neighbor not already covered by a relay node, is chosen as relay node. Relays are chosen until all 2-hop neighbors are covered. Each node signals its choice of relay nodes in its HELLO messages. Every node only forwards packets for neighbors that have explicitly chosen it as relay node.

Figure 1a gives a simplified example for SMF with NHDP and ETX. It shows a snapshot of a network after the relay set selection is done. The black lines represent the links in the network. Nodes A and B send correct HELLO messages. Node A propagates neighbors C,D and S with link quality and neighbor link quality 0.5 for each neighbor. This results in an ETX value of 4 for each propagated link. Node B propagates neighbors C, D, E and S with link quality 0.625 and neighbor link quality 0.8 for each neighbor. This leads to an ETX value of 2 for each propagated link. Hence, node S chooses node B as relay node. If node S sends data packets, only node B will forward these packets.

In order to run a sinkhole attack against SMF with NHDP and ETX, an attacker must fake HELLO messages, because they are used to provide the basic connectivity in the network. We consider an attacking node claiming to have high quality links to more neighbors than it actually has in its HELLO messages. In combination, the high quality of the attacker's links and his large number of neighbors lead to a high probability of the attacker being chosen as relay node, while other nodes are not chosen. By doing so, the attacker gains control of routes in the network. The more neighbors the attacking node claims to have and the better link qualities it propagates, the larger the potential impact of the attack. We note: There is a maximum impact achievable by the attacker. Of course, the more an attacker fakes, the larger the possibility of the attacker being detected.

Figure 1b shows the SMF network presented in Figure 1a, but this time node A has been taken over and launches a sinkhole attack. Node A propagates high quality links to nodes C, D, E and S (Label 1). Hence, node S does not choose node B, but node A as relay node (Label 2). Thus, node B does not forward data packets, but the attacker is responsible for forwarding these packets. Therefore, the attacker has gained control over the connection from S to C, D and E.

## 3 Related Work

There is only very little research done so far on detecting fake link qualities. Thus, in the following we mention not only related work dealing with fake link qualities, but also work at least being aware of link qualities.

[1] deals with securing the Pulse protocol against several attacks. The countermeasures include nonces, packet encryption and authentication. Against insider attacks, Awerbuch et al. use secure loss-rate information. By using cryptographic acknowledgements for each packet traversing a link, a secure loss-rate is determined for each link. These loss-rate information are used as a routing metric. Thus, a link quality based routing metric is introduced. Attacks against this routing metric are not considered in detail.

[15, 14] use intrusion detection to detect sinkhole attacks in wireless sensor networks. Several rules are defined to detect sinkhole attacks when using MintRoute or MultiHopLQI as routing protocol. Alteration of the attacker's link qualities is detected by plausibility checks. Each node acts as watchdog for its neighbors. It compares link qualities from incoming packets to link qualities propagated by other neighbors for the same links. If it detects a significant difference between claims of different neighbors, a fake link quality is assumed. This approach has two major drawbacks. First, without further processing it is only possible to indicate a sinkhole attack, but not to identify which node is launching the attack. Second, the approach requires the presence of watchdog nodes for each link. These watchdogs must be able to hear both nodes reporting a link between them. At least in a network with high mobility this requirement may be difficult to guarantee.

[19] defines a method to detect sinkhole attacks and identify the attacker in wireless sensor networks. It is assumed that data is transmitted to a base station consistently. Statistical methods are used to detect inconsistencies in data from a region. Upon detection of inconsistent data, a sinkhole is assumed. Thus, the base station initiates a procedure resulting in a flow graph for the suspicious region. The root of the biggest tree in the flow graph is assumed to be the attacker. The assumptions of this approach limit it to networks where traffic is transmitted to a base station consistently. Thus, the approach is not applicable to all kinds of multi-hop networks. In addition, fake link qualities are not considered.

[21] describes an algorithm to defend against selective forwarding attacks in wireless mesh networks. The detection happens in two phases. The first phase is threshold based. If for a given source-destination pair of nodes less than threshold packets are received by the destination node, a selective forwarding attack is assumed. The second phase is query based. The source node queries all intermediate nodes on the path to the destination. Based on their feedback, the attacker is determined. The detection threshold for the first phase is calculated according to the ETX metric. However, fake link qualities are not considered in this approach.

[15, 14] are the only approaches taking into account fake link qualities. However, these approaches are tailored to MintRoute and MultiHopLQI in wireless sensor networks, have some drawbacks (described above) and seem not applicable to tactical multi-hop networks. Thus, to the best of our knowledge, there are no approaches detecting fake link qualities in tactical multi-hop networks like our new approach TOGBAD-LQ does.

## 4 TOGBAD

In this section we present our approach Topology Graph based Anomaly Detection (TOGBAD). TOGBAD is a centralised anomaly detection method against routing attacks in tactical multi-hop networks. It uses the structure of tactical multi-hop networks by running the detection routines centrally on the fully equipped nodes. Preliminary versions were introduced in [7], [6] and are summed up in Section 4.1. In Section 4.2, we present our new extension TOGBAD-LQ.

## 4.1 Basic Functioning

TOGBAD utilizes two types of instances corresponding to the two types of nodes present in tactical multi-hop networks. The sensor instances of TOGBAD run on the light-weight nodes of the tactical multi-hop network. These nodes act as watchdogs and periodically send reports to a detection instance. From these reports the detection instances construct a graph modeling the topology of the network. The detection instances run on the fully equipped nodes of the multi-hop network. They perform plausibility checks between the actual topology represented in the topology graph and the topology propagated by nodes in the network. By doing so, the detection instances are able to detect nodes propagating fake topology. However, without enhancements this version of TOGBAD is not able to recognize fake link qualities. For further details concerning the basic functioning of TOGBAD we refer to [7].

## 4.2 TOGBAD-LQ

The basic idea of TOGBAD-LQ is to use a Challenge/Response method to estimate the link qualities in a node's neighborhood. The nodes include challenges in their messages. Based on these challenges, neighboring nodes create responses. These responses serve as basis for the estimation of link qualities. We will describe the Challenge/Response method in more detail below.

Each node checks the link qualities propagated by its neighbors against its own estimation of the link qualities. Upon detection of a suspicious link quality, a node sends a report to a fully equipped node. At the fully equipped node the reports on suspicious link qualities are aggregated and if the evidence is sufficient the sinkhole attacker is identified.

TOGBAD-LQ can be divided into two parts. The first is the local detection part. It consists of the estimation and checking of link qualities and the checking of neighbor link qualities. The second is the global detection part, where the local detections are aggregated and sinkhole attackers identified.

### 4.2.1 Local Detection

The local detection consists of two parts: (1) Estimation and checking of link qualities and (2) checking of neighbor link qualities. For (1), each node adds a challenge to its HELLO messages. Upon reception of a HELLO message containing a challenge, the neighboring nodes add a response to this challenge in their next HELLO message. From the number of received responses from a neighbor, a node can estimate the link quality of this neighbor. The number of received responses is used for the checking of link qualities. If the difference between number of received responses and number of expected responses according to the link quality propagated by the neighbor exceeds a threshold, a report is sent to a fully equipped node.

The challenges and responses should be chosen in a way that it is very difficult for an attacker to guess a correct response without the corresponding challenge. In particular, the challenges should be independent of each other. Thus, we use random values as challenges.

We will describe a way to derive responses below. Information from HELLO messages should not be taken as challenges, since successive HELLO messages of the same sender tend to be similar. To minimize the overhead introduced by our approach and to provide tamper-resistance, the responder sends back a hash-based message authentication code (HMAC) calculated from the received challenge. By use of a hash, the overhead is minimized and by using a message authentication code tamper-resistance provided.

The checking of link qualities is done in the following way: Each node maintains a list of challenges sent for a given time frame. Additionally, each node has a list of received responses for each neighbor in the given time frame. A received response is considered correct, if it corresponds to one challenge not already met by the neighbor sending the response from the list of challenges. Let $CS$ be the number of challenges sent in the considered time frame, B the node receiving a HELLO message and performing the check, A the sender of the HELLO message, $LQ_A$ the link quality measured by node A for the Link B→A, $LQ_B$ the link quality propagated by node B, $ER$ the number of expected responses and $RR$ the number of received correct responses to a challenge sent in the time frame.

$$ER := LQ_A * LQ_B * CS$$

$$local\_threshold := ER + \delta$$

A report is sent to a fully equipped node if

$$RR < local\_threshold.$$

The reports consist of a timestamp, the ID of the suspicious node, the ID of the reporting node and the difference between $local\_threshold$ and $RR$. In the following, this difference is named $diff$. The reports are added to the reports sent for the basic TOGBAD version, minimizing overhead and transmissions needed.

The checking of neighbor link qualities needs no additional signaling. It can be done completely locally. The neighbor link quality propagated by a neighbor is the link quality from a previous HELLO message of the node performing the check. Thus, to defend against fake neighbor link qualities, a node keeps a list of its previously propagated link qualities. To check the plausibility of a neighbor link quality propagated by a neighboring node, a node checks whether this neighbor link quality is present in its list of propagated link qualities for this neighboring node. Note that it is important to keep the lists of previously propagated link qualities short for two reasons: (1) to save resources of the nodes and (2) to reduce the probability of an attacker choosing a valid neighbor link quality. Please note that it is no problem if new nodes join in. New nodes will start transmitting neighbor link qualities for a neighboring node after they received at least one HELLO message advertising a link quality from this node.

### 4.2.2 Global Detection

The global detection is done at the fully equipped nodes. The approach works period-based. For a defined period the detector collects the reports sent by the watchdogs. At the end of the period, the detector aggregates all reports concerning one suspicious node received in the current period, calculates the mean over the $diff$ values from these reports and generates an alarm for a suspicious node, if

$$mean\_diff > global\_threshold.$$

To clarify our approach, we consider a simplified example (Figure 2). The example consists of three nodes. Node A is the attacker node, node B a benign node and node FE one fully equipped node. For this example, we set $CS := 10$, $RR := 2$ at node B, $\delta := -0.5$, $global\_threshold := 1$ and the link quality for link A-B := 0.5 in both directions. Thus, node B propagates a link quality and neighbor link quality of 0.5 for neighbor A in its HELLO message (Figure 2; Step 1). Additionally, node B adds a challenge to its message. Figure 2; Step 2 shows the subsequent HELLO message of the attacker node A. The attacker fakes the link quality and neighbor link quality and propagates the optimal value for both. Despite faking link quality and neighbor link quality, the attacker correctly includes the HMAC of node B's challenge as response in his HELLO message. Note that it would even simplify the detection of the attack if the attacker would not include responses in its HELLO messages. Upon reception of the attacker's HELLO message, node B first increments its $RR$ to 3. Afterwards, node B checks the propagated LQ and NLQ. In this case, $ER = 5$ resulting in $local\_threshold = 4.5$. Thus, node B sends a report with $diff = 1.5$ to the fully equipped node (Figure 2; Step 3). Additionally, node B checks the NLQ propagated by node A. For this example, we consider a list length of 1 for the previously propagated link qualities. Thus, node B compares the LQ of its last HELLO (0.5) to the NLQ of node A's HELLO (1.0). Since the values are unequal, the fake NLQ is detected. At the fully equipped node, the mean over all reports concerning node A is calculated and compared to the $global\_threshold$. In this case: $mean\_diff(A) = 1.5 > 1 = global\_threshold$ (Figure 2; Step 4). Thus, the fully equipped node generates an alarm for node A.

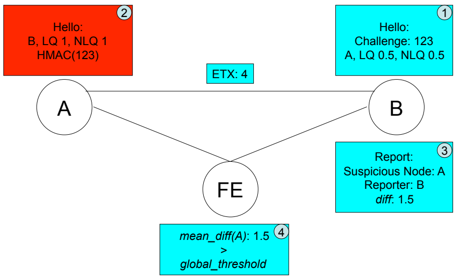


**Figure 2** Example for TOGBAD-LQ

## 5 Evaluation

To evaluate our approach, we conducted simulations. In this section, we first introduce the used simulation environment (5.1) and afterwards present our simulation (5.2) results.

### 5.1 Simulation Environment

For our simulations, we use the network simulator ns-2 [17] in version 2.33. Since ns-2 does not include an implementation of SMF, we added SMF with NHDP and ETX (cf. Section 2.4).

Since we consider tactical environments, we choose Reference Point Group Mobility (RPGM) [9] as mobility model. In tactical scenarios there typically are two kinds of communication channels present, intra-group and inter-group. The intra-group communication is mainly single-hop as the nodes of a group (at least when using RPGM) stay close together. Typically, the communication between tactical command and the troops in the field is inter-group and therefore multi-hop communication. In the following the inter-group communication channel is depicted as command channel. To guarantee multi-hop scenarios, the RPGM scenarios are generated with the additional criterion that one node at maximum may reach 50% of all nodes within one hop.

The military units of the RPGM scenarios utilize a tactical MANET that is attacked by a sinkhole in the simulations conducted. All nodes are equipped with radio hardware with a maximum communication range of approximately 300m. A combination of log-distance and ricean fading is used as signal propagation model. All packets are sent with a transfer rate of 11Mbps and are routed by applying the Simplified Multicast Forwarding (SMF) protocol with NHDP and ETX (cf. Sect. 2.4). The modelled military mission consists of several squads of infantry soldiers that are moving in an area of 1000m x 1000m. Each RPGM group consists of 10 nodes, which approximates the size of a military squad. The maximum distance between a unit and its corresponding group center is set to 300m to model a closely operating infantry squad. The total node number is set to 50. 400 replications of length 1000 seconds are done with varying movements and traffic. Additionally, only replications with a non-partitioned network for at least 90% of the simulation time are considered, since we assume that in a real tactical network some kind of topology control is in use.

From the 50 nodes simulated, we uniformly choose one attacker. The attacker sends fake HELLO messages. In these messages he propagates a fake topology and fake link qualities. According to the results of [7], the attacker propagates two-thirds of the total nodes as fake neighbors. Additionally, he sends optimal link qualities and neighbor link qualities for all propagated neighbors (real and fake ones). The attracted traffic is dropped by the attacker. The attacker is active between seconds 100 and 500. The rest of the simulation, the attacker node behaves like a normal one.

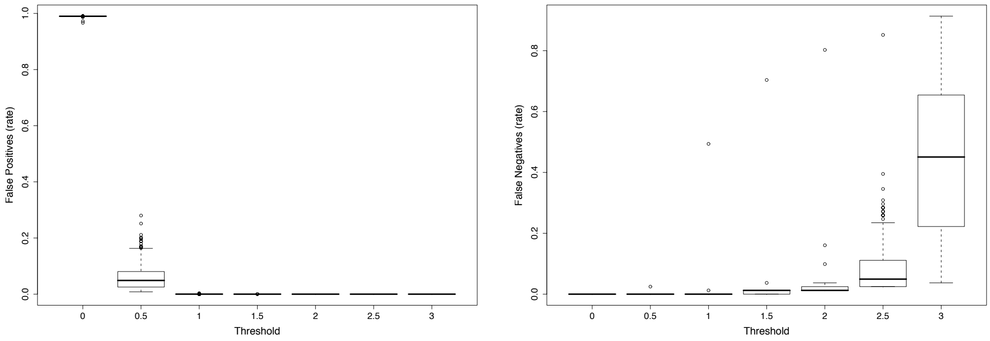
The report interval for TOGBAD should be chosen in dependency of the used HELLO interval. According to [4] we use a HELLO interval of 2 seconds. In [7] a report interval of 5 or 6 seconds was evaluated to work well given the above HELLO interval. In this work, we consider a report interval of 5 seconds. The detection of fake link qualities is done every 5 seconds, accordingly. Consequently, the interval for ETX determination should also be chosen in dependency of the HELLO interval. At least 10 HELLO messages should be evaluated for ETX determination. Thus, we consider an interval of 20 seconds. For plausibility checks of propagated link qualities and neighbor link qualities, only information from packets being considered for ETX determination are of interest. Therefore, each node stores its link qualities and challenges sent for 20 seconds.

## 5.2 Simulation Results

Concerning our simulation results, we start with an evaluation of a reasonable choice for the *global_threshold*. For this evaluation, every node sends a report to a fully equipped node, if the difference between *local_threshold* and $RR$ is greater than zero. Afterwards, we consider the impact of bursty packet losses on the detection rate of our approach.

To find a reasonable choice for the *global_threshold*, we consider the rate of false positives and false negatives of our approach in dependency of the different choices for the *global_threshold*. We choose the *global_threshold* out of the set $\{0; 0.5; 1; 1.5; 2; 2.5; 3\}$. At first, we consider an idealized situation: We assume that the reports of our sensor instances are not hit by packet losses. Thus, we have an optimal information base at the detector instance. The impact of packet losses of the reports is evaluated later (Fig. 4).

Figure 3a shows the rate of false positives over different choices for the *global_threshold*. We use boxplots to show the median, lower and upper quartile. For a *global_threshold* of zero, our approach leads to a median false positive rate of almost 100%. But already the choice of 0.5 for the *global_threshold* reduces this rate to around 10%. A choice of 1 or greater leads to a median false positive rate of 0%. The very high false positive rate for small choices of the *global_threshold* is due to packet losses in the network. Packet losses may lead to small differences between the measured and real link quality. Thus, there are reports with $diff$ values slightly above zero for correctly behaving nodes. Given a *global_threshold* close to zero, these reports lead to a high number of false positives. For more reasonable



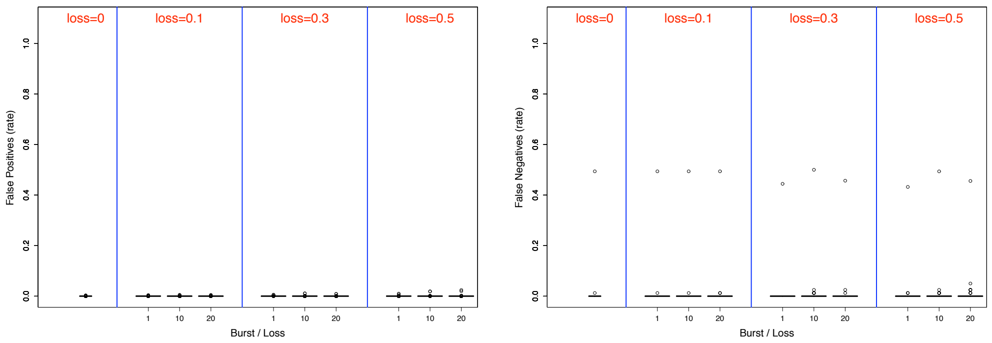
**(a)** False Positives

**(b)** False Negatives

**Figure 3** False Positives, False Negatives without packet loss for different global thresholds

choices of the *global_threshold*, these false positives disappear. Figure 3b uses boxplots to illustrate the rate of false negatives over different choices for the *global_threshold*. For small choices of the *global_threshold* the median false negative rate stays at 0%. From a choice of 1.5 the median rate of false negatives slightly increases up to 5% for a choice of 2.5 for the global threshold. The choice of 3 for the global threshold leads to a median false positive of 40%. The link quality of the majority of links in the considered scenarios is around 0.7. Given that the $global\_threshold \geq 3$, with high probability even a node propagating optimal link qualities (1.0) is considered correctly behaving. This leads to the high number of false negatives given $global\_threshold \geq 3$. According to Figure 3 $global\_threshold = 1$ is a reasonable choice. It leads to low false positives and false negatives rates and thus a very good detection rate. Hence, in the following we use a *global_threshold* of 1. There are few outliers in Figure 3b. Given a reasonable choice for the *global_threshold*, two conditions may lead to a high false negative rate: (1)very high link qualities in the direct neighborhood of the attacker node and (2)attacker node nearly exclusively reaches members of its movement group directly. Condition (1) leads to a low difference between the real link qualities and the fake link qualities propagated by the attacker. Condition (2) leads to a small number of watchdogs reporting over the attacker. The outliers visible in Figure 4 are the cases where Conditions (1) and (2) occur simultaneously. Nevertheless, the probability of both conditions occuring simultaneously is very low.

Figure 4 shows the impact of bursty packet losses on the detection rate of our approach. To model the bursty packet losses, we use a two-state Markov chain [18] with states loss and no loss. We vary packet loss rate and average burst length to measure both the impact of increasing packet loss rate and burst length. In Figure 4a the false positive rate is visualized over different loss rate/burst length combinations. Neither with increasing loss rate, nor with increasing burst length the rate of false positives increases significantly. The median of the false positive rate stays at 0% for all combinations. Only the number of outliers increases with increasing loss rate and burst length. Figure 4b illustrates the false negative rate over different loss rate/burst length combinations. Like the false positive rate, the false negative rate is very robust against both, increasing loss rate and increasing burst length. The median false negative rate stays at 0% for all loss rate/burst length combinations. Again, the number of outliers increases with loss rate and burst length. Figure 4 shows that our approach is very robust against packet losses. In tactical scenarios group based movement is to be expected.



**(a)** False Positives

**(b)** False Negatives

**Figure 4** False Positives, False Negatives with packet loss for a global threshold of 1

Due to the group based mobility each node has with high probability at least the members of its group as direct neighbors. Thus, -in the considered scenarios with a group size of 10 nodes- for each node there are with high probability at least 9 nodes reporting about its behavior. Even if 50% of the reports of these reporting nodes are hit by packet losses, there is a high probability of at least some of the reports reaching the detection instance. Already a small number of reports is sufficient to reach a very good detection rate.

## 6 Conclusion and Future Work

In this paper we introduced a new detection capability for fake link qualities to our intrusion detection approach TOGBAD. TOGBAD-LQ uses a Challenge/Response method to estimate link qualities in the neighborhood of nodes. Based on this estimation, first, a local plausibility check is performed. The results of these local plausibility checks are then aggregated at a central detection instance. This approach takes advantage of the characteristics of tactical environments by running the central detection instances on the fully equipped nodes in the network.

We considered an attacker launching a sinkhole attack by propagating fake topology and link qualities. To detect this attack, we evaluated a reasonable threshold for our approach. Given a reasonable choice for the required thresholds, our approach shows very good results. It leads to very few false positives and false negatives and was shown to be very robust against packet losses. In total, it reliably detects fake link qualities in tactical scenarios.

However, there are still questions which have to be examined in the future. An evaluation for a reasonable choice of the local threshold should be performed. Additionally, the overhead introduced by our approach has to be evaluated. Furthermore, the impact and detection of an attacker only slightly increasing its link qualities should be considered.

## 7 Acknowledgments

This work was supported in part by the State of North Rhine-Westphalia within the B-IT Research School.

## References

1 B. Awerbuch, *et al.*, “Secure Multi-Hop Infrastructure Access,” *Proc. of Network and Distributed System Security Symposium (NDSS)*, 2005.

2 T. Clausen, *et al.*, “IETF Draft MANET Neighborhood Discovery Protocol,” *http://www.ietf.org*, 2009.

3 ——, “IETF Draft The Optimized Link State Routing Protocol version 2,” *http://www.ietf.org*, 2009.

4 T. Clausen *et al.*, “RFC 3626 Optimized Link State Routing Protocol (OLSR),” *http://www.ietf.org*, 2003.

5 D. de Couto, *et al.*, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” *Proc. of ACM Conference on Mobile Computing and Networking (MobiCom)*, 2003.

6 E. Gerhards-Padilla, *et al.*, “Enhancements on and Evaluation of TOGBAD in Tactical MANETS,” *Proc. of the 27th Military Communication Conference (MILCOM)*, 2008.

7 ——, “TOGBAD - An Approach to Detect Routing Attacks in Tactical Environments,” *accepted for Wiley Security and Communication Networks*, 2010.

8 M. Gerharz, “Stabile Kommunikation in Dynamischen Ad-hoc-Netzwerken,” *GCA-Verlag*, 2006, Doctoral Thesis University of Bonn.

9 X. Hong, *et al.*, “A group mobility model for ad hoc wireless networks,” *Proc. of ACM Int. Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM)*, 1999.

10 Y.-C. Hu, *et al.*, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” in *Proc. of ACM Int. Conference on Mobile Computing and Networking (MobiCom)*, 2002.

11 ——, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” in *Proc. of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, 2003.

12 J. Hubaux, *et al.*, “The Quest for Security in Mobile Ad Hoc Networks,” in *Proc. of ACM Int. Symposium on Mobile ad hoc Networking & Computing (MobiHOC)*, 2001.

13 C. Karlof *et al.*, “Secure Routing in wireless sensor networks: attacks and countermeasures,” *Elsevier’s AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 4837/2008, no. 2–3, pp. 293–315, September 2003.

14 I. Krontiris, *et al.*, “Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks,” *Algorithmic Aspects of Wireless Sensor Networks*, vol. 48372008, 2008.

15 ——, “Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side,” *Proc. of IEEE Int. Conference on Wireless and Mobile Computing, Networking and Communication (WIMOB)*, 2008.

16 J. Macker, “IETF Draft Simplified Multicast Forwarding for MANET,” *http://www.ietf.org*, 2009.

17 S. McCanne *et al.*, “ns Network Simulator,” *http://www.isi.edu/nsnam/ns/*.

18 B. Milner *et al.*, “An Analysis of Packet Loss Models for Distributed Speech Recognition,” in *Proc. of the 8th Int. Conference on Spoken Language Processing (INTERSPEECH)*, 2004.

19 E. Ngai, *et al.*, “On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks,” *Proc. of IEEE Int. Conference on Communications (ICC)*, 2006.

20 S. Roy, *et al.*, “High-Throughput Multicast Routing Metrics in Wireless Mesh Networks,” *Proc. of IEEE Int. Conference on Distributed Computing Systems (ICDCS)*, 2006.

21 D. Shila *et al.*, “Defending Selective Forwarding Attacks in WMNs,” *Proc. of IEEE Int. Conference on Electro/Information Technology (EIT)*, 2008.