Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs *

Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini
University of Bonn, Institute of Computer Science IV
Römerstr. 164, D-53117 Bonn, Germany
{padilla, aschenbruck, martini}@cs.uni-bonn.de

Marko Jahnke, Jens Tölle
FGAN - FKIE/KOM
Neuenahrer Strasse 20, D-53343 Wachtberg, Germany
{jahnke, toelle}@fgan.de

***Abstract*— Black Hole Attacks are a serious threat to communication in tactical MANETs. In this work we present TOGBAD a new centralised approach, using topology graphs to identify nodes attempting to create a black hole. We use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network. We consider a node generating fake routing information as malicious. Therefore, we trigger an alarm if the plausibility check fails. Furthermore, we present promising first simulation results. With our new approach, it is possible to already detect the attempt to create a black hole before the actual impact occurs.**

I. Introduction

In tactical (i.e. used by military or civil protection) communication systems, sensitive data (e.g. information on soldier positions) is transmitted over a wireless network with a potentially high probability of enemies being around. Therefore, a secure and reliable communication is essential.

In tactical Mobile Ad Hoc Networks (MANETs), we assume that confidentiality, integrity, and authenticity of the transmitted packets are provided by cryptography. Excellent work is available in this field; e.g. refer to [1] for an overview of cryptographic methods providing encryption, checksums, signatures or access control. However, especially in tactical MANETs, it cannot be ultimatively precluded that nodes owning valid cryptographic keys are taken over by an attacker. Therefore, it is crucial to recognise whether a node – despite owning valid keys and recent correct behaviour – is behaving legitimately or maliciously.

There are different layers on which a node can behave maliciously. For example, an application may create fake traffic in order to run a denial-of-service attack. In this paper we focus on recognising nodes spreading illegitimate routing information. Recent related work focuses on securing existing ([2], [3]) or developing secure protocols ([4], [5], [6], [7], [1]) to prevent routing attacks or using intrusion detection ([8], [9], [1]) to detect such attacks.

In this paper we present a novel centralised intrusion detection approach for detecting routing attacks against the Optimized Link State Routing protocol (OLSR) [10] in tactical MANETs called Topology Graph based Anomaly Detection (TOGBAD). This new approach tries to detect falsified HELLO messages by performing plausibility tests at a central node against a topology graph.

The remainder of this paper is structured as follows. In section II we describe the characteristics of tactical MANETs, in particular the differences between ordinary and tactical MANETs. Section III describes routing attacks in general and their specific implementation in OLSR. Section IV presents some related work regarding prevention and detection of routing attacks. We introduce the new detection approach TOGBAD (sect. V). Next, first simulation results are shown (sect. VI). Finally, we conclude the paper and point out future work in section VII.

II. Tactical MANETs

According to [11], a MANET in general has the following characteristics:

- dynamic topology due to node mobility,
- limited bandwidth due to wireless communication,
- limited energy resources due to battery powered devices, and
- limited security against eavesdropping, since communication is done across an intrinsically open medium.

Tactical MANETs are specialised for being used in military scenarios (e.g. infantry missions) or in disaster areas where existing communication infrastructure may have been destroyed. Similar to general MANETs, a tactical MANET has a dynamic topology, low bandwidth and limited security. Typical applications in tactical MANETs are voice communication as well as command & control systems which e.g. process and transmit geographic and topologic information of the operational area or tactical commands for the units.

There is typically some kind of hierarchical command structure in tactical MANETs which implies at least two types of nodes: supervising nodes and supervised nodes. These types differ especially in their geographic position and employed hardware. Supervising nodes typically stay in the background, have access to a power supply, and therefore can use more powerful hardware. In contrast to that, the supervised nodes move frequently, use battery powered handhelds and therefore less powerful hardware. The powerful hardware of the supervising nodes predestines them to serve as central instances in securing the network. TOGBAD utilises the supervising nodes for composing topology graphs and performing plausibility checks.

* Published in: Proc. of the 3rd LCN Workshop on Network Security. Held in conjunction with the 32nd IEEE Conference on Local Computer Networks (LCN), Dublin, Ireland, Oct. 2007.

III. Routing Attacks

In MANETs, every node participates in the routing process. Hence, it is possible for attackers to launch attacks against the routing protocol by sending false routing information. The possibility of such attacks was already mentioned in [12]. In [6] these attacks against the routing protocol are referred to as *routing disruption attacks*. By sending false routing information, an attacker may try to dispose other nodes to make him a part of their routes. This is often referred to as 'route attraction'. If an attacker succeeds in attracting routes, he may perform several attacks (cf. [13]), including

- eavesdropping messages,
- selectively dropping data,
- manipulating data, or
- launching a denial-of-service (DoS) attack.

Like in [13], we assume protection against eavesdropping and manipulation by means of cryptography. Additionally, selective dropping of data is a special case of a DoS attack. Furtheron, we focus only on these kinds of attacks.

A. Black Hole Attack

There are several examples of DoS attacks against routing protocols. A black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. Additionally, a special case of the black hole attack called gray hole attack is mentioned in [6]. In this case some packets are discarded (e.g. application data) while others are forwarded (e.g. routing packets). In the literature (e.g. [14], [15] and [13]) there are similar definitions of black and gray hole. However, a gray hole is only a special case of a black hole that has similar impact but is harder to detect. In the following, we will without limitation of generality focus on an attacker forwarding routing packets and dropping application data packets. We will refer to this attack as black hole attack.

The actual implementation of the black hole attack strongly depends on the deployed routing protocol. In this paper, we focus on OLSR because it is standardised ([10]) and widely in use. However, in the future we plan to adapt the approach for other routing protocols as well.

B. OLSR

Optimized Link State Routing (OLSR) is specified in RFC 3626 [10]. It is classified as a 'pro-active' routing protocol, due to its periodically spreaded routing information. The core optimisation of OLSR – compared to traditional link state routing – is the dissemination of link state information only by a subset of MANET nodes called Multipoint Relays (MPRs). MPRs are chosen from the neighbours of a node such that connectivity to all known nodes in 2-hop distance of the node can be assured.

In OLSR there are four different kinds of messages:

- HELLO messages,
- Topology Control (TC),
- Multiple Interface Declaration (MID),
- Host and Network Association (HNA).

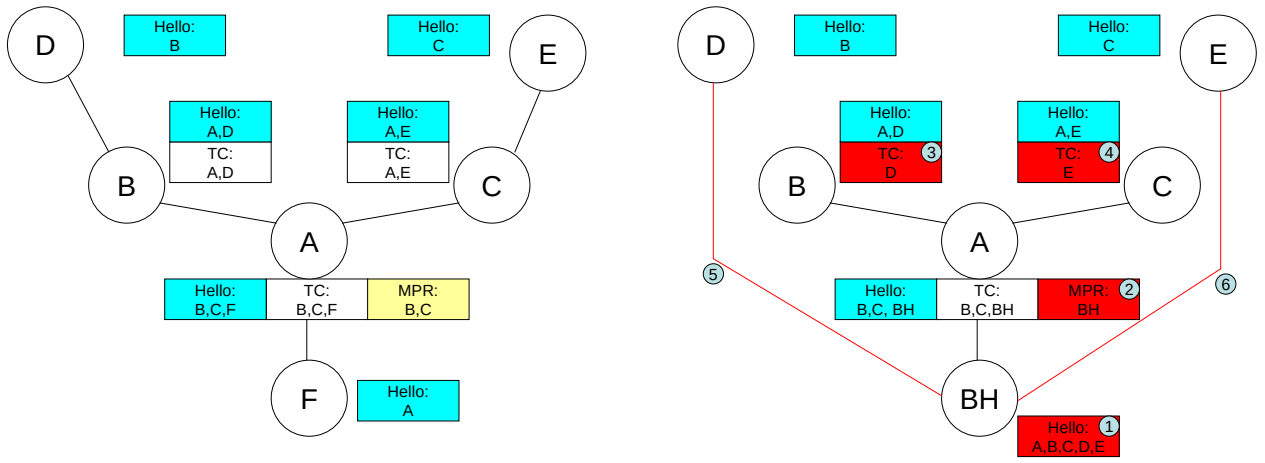
HELLO messages are used for link sensing, neighbour detection and MPR signalling. Such a message contains information about the local links, neighbours of a node, and it tells the receiving node whether it was chosen as an MPR. Their scope is restricted to one hop. TC messages perform topology declaration by advertising link states. They are spread across the network via the nodes selected as MPRs. MID messages declare the presence of multiple interfaces on a node. Only nodes with more than one interface create MID messages. These messages are spread across the network using the MPRs. HNA messages are used to provide connectivity between non-OLSR and OLSR interfaces. They are also propagated in the network via the MPRs.

Figure 1(a) shows a static OLSR network once the routes have been established. For simplicity, in this example we focus on Hello and TC messages spreaded by the nodes. Additionally, we show the nodes chosen as MPRs by Node A. The black lines represent the available routes and the ones usable by node A. Without black hole there is no difference between node A's view of the network and the existing routes, since all nodes propagate correct messages. For example, Node A reports its neighbours B,C,F in its Hello messages, its MPR selectors B,C,F in its TC messages and chooses its neighbours B,C as MPRs. For further details see [10].

C. Black Hole Attack in OLSR

In order to run a DoS attack against OLSR, it is reasonable to fake HELLO and/or TC messages, because they are used to provide the basic connectivity in the network. The first possibility is faking only TC messages. This is not reasonable because it is possible to detect a fake TC message by means of local plausibility checks (cf. [9]). The second possibility is to fake both HELLO and TC messages. This approach is not chosen in this work, as a single node receiving a TC message including its address while not considering the originator, a neighbour will be able to detect the attack. We implemented a third approach. A node acting as black hole sends fake HELLO messages. In these messages an attacking node claims to have links to more neighbours than it actually has. Thus, there is a high probability that this node is chosen as an MPR by its neighbour. The more neighbours the attacking node claims to have, the larger the potential impact of the attack. Due to the fake messages of the attacker, in its neighbourhood falsified TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture routes.

Figure 1(b) shows the OLSR network presented in Figure 1(a). This time node F has been taken over and acts as black hole. This leads to some changes in the network. In this figure, the lines just show Node A's view of the network. Change Nr. 1 is the fake Hello message of the black hole node. It contains nodes A,B,C,D and E. This leads to Node A selecting only the black hole node as MPR (Change Nr. 2). Since Node A does not select nodes B,C as MPRs, these send TC messages not



(a) OLSR without Blackhole

(b) OLSR with Blackhole

Fig. 1. Example for OLSR

containing Node A (Changes Nr. 3, 4). Additionally, instead of sending data packets to nodes D,E via nodes B respectively C, node A tries to send these data packets via the black hole node (Changes Nr. 5,6). Therefore, the black hole has gained control over the connections from A to D and E.

IV. Related Work

As mentioned, the research conducted so far may be divided into three categories: securing existing protocols, developing new secure protocols, and intrusion detection techniques. The works by Hong et al. [2] and Raffo et al. [3] deal with securing OLSR. In [2] OLSR is secured by using hash chains and digital signatures. Nodes owning valid keys and behaving maliciously are not considered. [3] presents a signature based approach for securing OLSR. A node reporting a link to a second node must – if possible – provide a proof for its claim. This proof is based on a previously received message of the neighbour. For example, if node A reports a symmetric link to a neighbour B, it must previously have received a message of this neighbour B declaring an asymmetric or symmetric link to A. The proof includes a timestamp and a signature calculated using information from node B's message. In this way, link spoofing is prevented. This approach requires the addition of a new kind of messages to OLSR which has to be sent with each HELLO and TC message.

In [4], [5], [6] and [7], new protocols are designed. Awerbuch et al. [4], [16] developed a secure new on-demand routing protocol. It includes link weights which are considered during route discovery. The weights are calculated from the packet delivery fraction of each link. A link not delivering a fraction of packets above a certain threshold is considered malicious, and therefore the link weight is increased such that the link is chosen with smaller probability in the next route discovery phase. The approach detects a black hole as soon as the impact occurs, not when the black hole is constructed. Deng et al. [5], [17] present an intrusion-tolerant approach for wireless sensor networks. The computation of routing tables is performed at a base station with a central view of the whole network. To achieve intrusion tolerance, not only one route from source to destination is used but redundancy is employed. This approach is applicable for defence against DoS attacks, but not against eavesdropping. In [6] a secure routing protocol based on the Dynamic Source Routing (DSR) protocol is presented. The authenticity of Route Requests is verified using message authentication codes (MAC). Furthermore, the authors present three techniques for authenticating data in Route Requests and Route Replies. Either a broadcast authentication protocol for authenticating routing messages called TESLA ([18], [19]), digital signatures or MACs are used. Additionally, the authors propose per-hop hashing to verify that no node present in the node list of the Route Request is removed by an attacker. Finally, similar to [4] routes are chosen with regard to their prior performance in packet delivery. The work focuses on on-demand protocols. Therefore, their approach is not applicable to proactive protocols. Papadimitratos and Haas [7] propose a secure link state protocol. Information from advertised link state messages is only accepted if both nodes of a link report the same state of the link within a given interval. The delay immanent to this approach is critical. Even with no enemies being present, there is a delay in the route discovery process.

[8] and [9] use intrusion detection to counter routing attacks. [8] introduces a system combining certificates to provide authenticity and integrity with intrusion detection to identify misbehaving nodes. Intrusion detection is used, but [8] focuses on the combination of certificates and intrusion detection, the detection process is just roughly specified. In [9] an intrusion detection approach for OLSR is proposed. Based on the intrinsic properties of OLSR messages, local plausibility checks are performed. In this way, falsified TC messages can be detected. However, falsified HELLO messages can not be detected.

The work of Kargl [20], [1] covers the development of a new

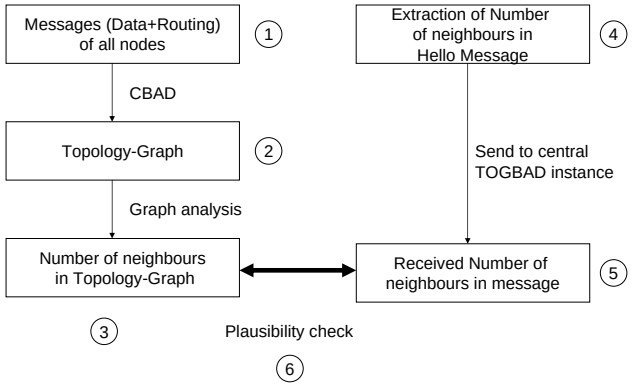


Fig. 2. Algorithm of TOGBAD

secure routing protocol as well as the usage of intrusion detection to detect node misbehaviour. The new protocol Secure Dynamic Source Routing (SDSR) is based on DSR. It provides authentication of nodes and integrity of routing packets by using cryptography, but is not secured against nodes dropping packets. The threat of packet dropping is dealt with by an intrusion detection system called Mobile Intrusion Detection System (MobIDS). MobIDS is a distributed approach. Each node in the network runs a MobIDS instance and manages ratings for the other nodes. The ratings are adjusted depending on the reports of the sensors employed by MobIDS and spread to neighbour nodes. Kargl's approach is not directly applicable to OLSR. The securing of DSR can not be ported to OLSR as it is only deployable with on-demand protocols. Additionally, a distributed intrusion detection system is not able to detect all kinds of fake HELLO messages.

V. TOGBAD

In this section we describe our centralised topology graph based approach called TOGBAD. The approach consists of three parts. In part one, a topology graph is created and the number of neighbours of a node according to this topology graph is calculated. (Fig. 2; step 1-3) In part two, the number of neighbours a node claims to have in its HELLO messages is determined. (Fig. 2; step 4,5) Finally, in part three, for each HELLO message, the originator's number of neighbours according to the message is checked for plausibility against the number of neighbours according to the topology graph. (Fig. 2; step 6) A significant difference between the two values triggers an alarm.

A. Calculating Number of Neighbours

The topology graph is obtained by using a modified version of the Cluster-Based Anomaly Detector (CBAD) presented in [21], [22]. CBAD was originally designed as an anomaly detector for wired networks. Based on received packets CBAD creates graphs representing a traffic structure. Significant changes in this structure are considered as indications of attacks.

CBAD follows a round-based approach. One round lasts a user-defined period and for each round, a graph is created. The graph of the current round is compared to graphs from previous rounds. If the difference between the graphs exceeds a threshold, an alarm is triggered. The basic graphs are created in the following way: After receiving a packet, a node – if not already present in the graph – is created for source address and destination address of the packet. Furthermore, an edge between the two nodes is inserted. Thereafter, CBAD employs clustering algorithms to obtain the typical traffic structure of the network. Our approach differs in this part, since we do not use clustering. Thus, we omit further details concerning clustering in CBAD and refer to [21] and [22] for further details.

In traditional wired networks, CBAD uses a global view of the network. In MANETs, this kind of view is not easy to achieve. Earlier work [23] has presented promising approaches for distributed traffic sensors in MANETs. We assume a set of traffic sensors that covers the whole MANET, sending statistics messages to our central analyser station. In a preprocessor stage, duplicates due to radio range overlaps are detected and purged.

There are two modifications to CBAD which lead to the construction of a topology graph, i.e. a graph containing complete topological information of the network.

a) Consideration of routing and data packets
b) Consideration of all hops
} Fig.2; step 1

Traditional CBAD considered only source and destination address of data packets. Neither routing packets nor intermediate nodes were present in CBAD's graphs. The additional consideration of routing packets and intermediate nodes leads to all nodes participating in the network being present in the graphs created by CBAD given the assumption that CBAD's round length is appropriately chosen. The modified version of CBAD provides the topology graphs our approach needs (Fig. 2; step 2). CBAD's round length should be chosen at least greater than OLSR's HELLO interval. Otherwise it cannot be assured that all nodes are present in one CBAD graph. Given this lower bound, there is a trade-off between resource consumption and precision: The round length should not be chosen too large, since the graph is a static representation of a dynamic network. Therefore, its precision decreases with large round lengths. On the other hand, small round length yield frequent computation of graphs. In tactical MANETs, we consider detection precision more important than economical resource usage, because a successful attack can lead to a failed mission and even to human losses. Thus, we use a round length of $2 * TC\_interval = 10$ seconds.

In the topology graph, each network node is represented by a node and each link is represented by an edge. Therefore, the degree of each node is the number of neighbours we are looking for (Fig. 2; step 3).

The number of neighbours claimed in propagated HELLO messages is determined in the following way: Every network node extracts the number of neighbours from a received HELLO message (Fig. 2; step 4) and sends the information to the central TOGBAD instance running on a supervising node.

B. Detecting Misbehaviour

The core part of TOGBAD is responsible for detecting routing misbehaviour. If the central TOGBAD instance receives a message from one of the network nodes, it extracts the number of neighbours for the originator of the HELLO message from the Topology Graph (Fig. 2; step 3) and checks the plausibility (Fig. 2; step 6) by comparing this number to the number of propagated neighbours (Fig. 2; step 5). A significant difference between propagated neighbours and neighbours in the graph is classified as an attack attempt and an alarm is triggered.

TOGBAD uses two formulae for detecting misbehaviour. Let o be the originator of a routing message, then

$$t(o) = \text{node degree in topology graph}$$

and

$$m(o) = \text{number of neighbours in routing message.}$$

Under ideal circumstances, we expect:

$$t(o) = m(o)$$

Taking into account the dynamic nature of MANETs, we assume:

$$t(o) = m(o) + \delta$$

where δ represents the deviation due to node movement. If TOGBAD discovers $t(o)$ significantly smaller than $m(o) + \delta$

$$t(o) << m(o) + \delta$$

an alarm is triggered. One of the remaining questions is when to consider a deviation "significantly" smaller. In our approach we use a threshold based approach. Let

$$\textit{diff} := m(o) + \delta - t(o)$$

If

$$\textit{diff} > threshold$$

an alarm is generated. The threshold determination strongly depends on the specific network. It may be based on several metrics, e.g. average of previous *diff* values or maximum of previous *diff* values. The determination of an effective and efficient method to determine the metric is one subject for future work.

VI. Simulation

In this section, we discuss early simulation results. The aim is to show basic functionality and point out the benefit of our new approach. First, we describe the scenarios and simulation environments. After that, we present the obtained results.

A. Scenario and Simulation Environment

The simulation results were obtained using version 2.29.3 of the network simulator ns-2 [24]. We modified the standard 2.29.3 version of ns-2. Since ns-2 does not include an implementation of OLSR, a RFC compliant implementation of OLSR [25] was added.

Since the presented simulations just account for the basic functionality of our approach, we decided to present a static scenario and a scenario with nodes moving according to the random waypoint mobility model. We are aware of the drawbacks (cf. [26], [27]) of the random waypoint model regarding decreasing mobility and high node density at the centre of the simulation area. Additionally, we assume an initial phase of 5000 seconds to ensure that the random waypoint model reached a steady state. However, we wanted to evaluate our approach under general conditions. Furthermore, high node density may be regarded as a difficult condition for our approach. Therefore, random waypoint may be considered as a kind of disadvantageous case.

We consider 25 nodes on a 1000 m x 1000 m area. Each node has a transmission range of 200 m. The total simulation time is 550 seconds, after an initial phase of 50 seconds. Four senders and four corresponding receivers are randomly chosen. The traffic is constant bit rate with each sender transmitting one packet every 0.51 seconds starting at 0.1 seconds of simulation time. One node attempts to launch a black hole attack at simulation time 150.1 seconds and stops at 350.1 seconds. During this time, it sends fake HELLO messages containing 24 neighbours. 24 is chosen because the attacker tries to route as much traffic as possible through himself. Before and after acting as black hole, the node behaves correctly. In the static scenario, the nodes are randomly distributed over the simulation area. Node 0 launches a black hole attack. In the mobile scenario, the nodes move according to the random waypoint model with a minimum speed of 0.5 m/s (1.8 km/h) and a maximum speed of 2.0 m/s (7.2 km/h) approximating pedestrian speed. Again, node 0 launches a black hole attack. For each scenario we generated ten different node distributions and movement patterns, respectively.

B. Results

This section shows the simulation results. We performed ten simulations using static scenarios and ten simulations with mobility. Figure 3 shows the average packet delivery fraction (pdf) of the static scenario with 0.95 confidence intervals calculated over the ten replications. The pdf is calculated over intervals of five seconds. It remains at 100% until the black hole attack is launched. A few seconds after the black hole node starts sending fake routing information the average pdf drops to 75% and remains at about 75% percent until the black hole is switched off again. Approximately 15 seconds after the black hole attack is switched off, the pdf raises back to 100%. There are big confidence intervals when the black hole attack is switched on. The reason for this and the average pdf not dropping to a value smaller than 75% is that a black hole in OLSR has only local impact in the respect that the

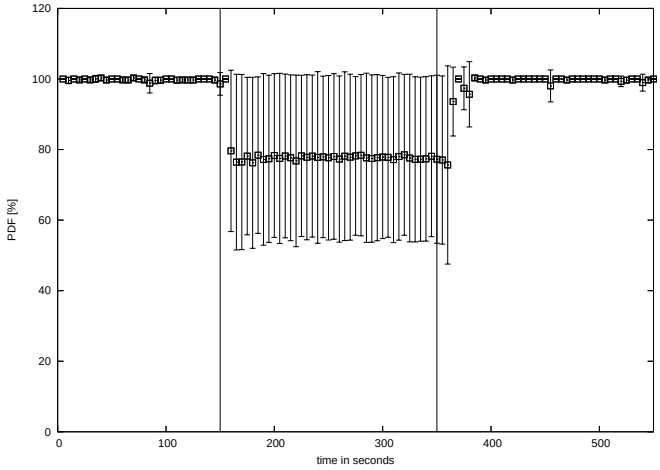


Fig. 3. Packet Delivery Fraction (PDF) in Static Scenario

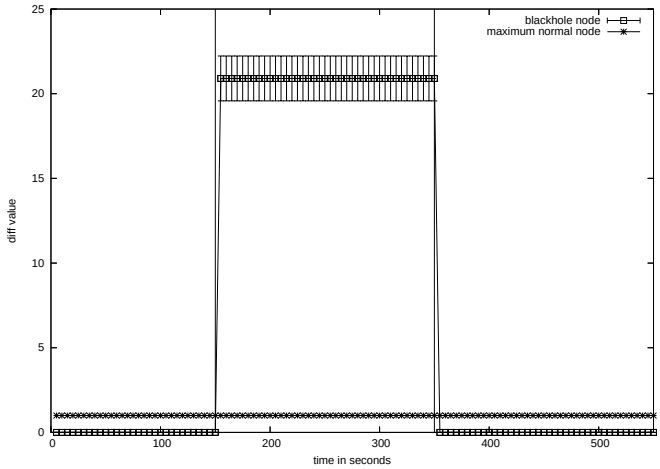


Fig. 4. *diff* value in Static Scenario

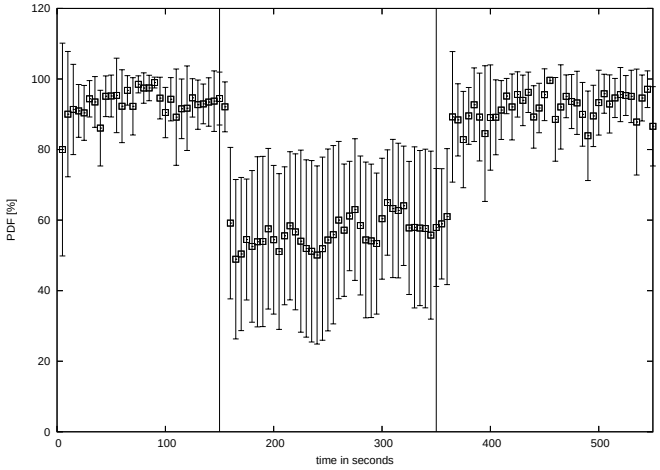


Fig. 5. Packet Delivery Fraction (PDF) in Mobile Scenario

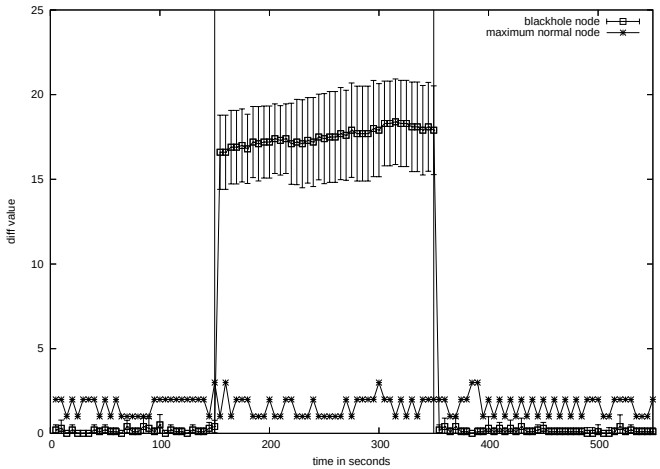


Fig. 6. *diff* value in Mobile Scenario

route propagated by the black hole must be at least as short as a concurring non-fake route. Additionally, due to the random node distribution the position of the black hole is randomly based. Thus, there are scenarios where the black hole node is in the centre of the simulation area, influencing a big number of nodes with high probability and scenarios where the black hole node is at the border of the simulation area, influencing a small number of nodes with high probability. This explains the large confidence intervals.

There is a small delay between the time the black hole attack is switched on (respectively is switched off) until the impact on the pdf may be noted. When the black hole is switched on the fake HELLO messages and the wrong TC messages resulting from them have to be spread until an impact on the pdf is visible. Similar to this the valid routing messages have to be spread when the black hole is switched off. Additionally, timeouts for the old routes are necessary for OLSR to consider the routes invalid.

In Figure 4, the *diff* values (see sect. V-B) over time in the static scenario are shown. We calculated average and 0.95 confidence interval over five second intervals over the ten replications for the black hole node. Over all nodes excluding the black hole node and over all replications, we calculated the maximum *diff* values over five second intervals. There are two different graphs present in this figure. The first shows the maximum *diff* value of all replications for each interval for non-black hole nodes. The second graph shows the average *diff* values with 0.95 confidence intervals of the black hole node. Since there is no mobility in this scenario, the network topology does not change. Therefore, the maximum *diff* values for non-black hole nodes remain very small. After the black hole attack is launched, the black hole node has an average *diff* value of nearly 21 until the attack is switched off again.

In Figure 5, we present the pdf for the mobile scenario. Again, we calculated average and 0.95 confidence intervals over five second intervals over the ten replications. Without black hole the average pdf stays mainly at about 90%. Compared to the static scenario the pdf stays at a lower value due to the mobility of the nodes. Note that there are big confidence intervals, in this scenario not only when the black hole is

active, but also with all nodes behaving correctly. This is due to node movement and to the local impact of a black hole attack already seen in the static scenario. Nevertheless, the average pdf drops to about 60% when the black hole is switched on. Furthermore, the average pdf again drops (increases) about 15 seconds after the black hole is switched on (off), similar to the static scenario. This is caused by the time necessary for spreading the fake (valid) routing messages.

Figure 6 presents the *diff* values of the mobile scenario. Like in the grid scenario, the average *diff* values and 0.95 confidence intervals of the black hole node and the maximum *diff* values for non-black hole nodes are calculated over 5 second intervals and all replications. The maximum *diff* values for non-black hole nodes reach at most a value of three. While the black hole attack is active, the average *diff* values of the black hole node are larger than 15. Thus, for the entire duration of the black hole attack the *diff* value of the black hole node is significantly larger than the maximum over all non-black hole nodes.

In general, TOGBAD succeeds in detecting black hole attacks against the OLSR protocol. In both scenarios, static and mobile, the average pdf dropped when the black hole attack was switched on. The black hole had a clearly visible impact. Nevertheless, due to the big and overlapping confidence intervals further examination is needed. Also in both scenarios, there was a delay until the impact of switching on/off the black hole was visible. The average *diff* values of the black hole node during the time the black hole was switched on were significantly bigger than the maximum *diff* values of the non-black hole nodes. The *diff* values changed immediately after the black hole was switched on. Thus, with our approach it is possible to detect a black hole attack immediately when it is launched and not when the effect occurs.

VII. Conclusion and Future Work

In this paper we presented our novel approach, TOGBAD, for detecting routing attacks in tactical MANETs. TOGBAD takes the characteristics of tactical MANETs into account in the way that a centralised approach – according to a hierarchical command structure – is used. Topology information is gained and represented in topology graphs. Based on this, plausibility checks for propagated routing messages are performed. First promising simulation results are presented which show the potential of our approach.

However, there are still questions remaining which have to be examined in the future. The amount of traffic overhead generated has to be examined. Furthermore, attacks against TOGBAD itself (e.g. malicious nodes sending spoofed messages or nodes modifying messages) have to be considered. Additionally, the black hole may influence the messages needed to build the topology graph, because also for these messages routes are needed. This point also has to be addressed.

Besides the issues already mentioned, we plan to further evaluate the approach, especially involving realistic mobility and traffic models suitable for tactical MANETs. In addition, the development of a robust metric to determine whether a *diff* value leads to the creation of an alarm, is necessary. Furthermore, we plan to evaluate TOGBAD using routing protocols other than OLSR.

Acknowledgement

Parts of this work have been sponsored by the Federal Office for information management and information technology of the German Federal Armed Forces (IT-AmtBw). The authors would like to thank the MITE cooperation project team and especially Anne Diefenbach, for the sustainable discussions and work.

References

[1] F. Kargl, "Sicherheit in Mobilen Ad hoc Netzwerken," Ph.D. dissertation, Universitaet Ulm, 2003, [in German].

[2] F. Hong, L. Hong, and C. Fu, "Secure OLSR," *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, 2005.

[3] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for OLSR," *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, 2004.

[4] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2002.

[5] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Rep. CU-CS-939-02, 2002.

[6] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking*, 2002.

[7] P. Papadimitratos and Z. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," *Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks*, 2003.

[8] R. Puttini, R. de Sousa, and L. Mé, "Combining Certification-based Authentication and Intrusion Detection to Secure Manet Routing Protocols," *Proceedings of the 5th European Wireless Conference (Mobile and Wireless Systems beyond 3G)*, 2004.

[9] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for OLSR MANET protocol," *Proceedings of 1st IEEE ICNP Workshop on Secure Network Protocols*, 2005.

[10] T. Clausen and P. Jacquet, "RFC 3626 Optimized Link State Routing Protocol (OLSR)," 2003.

[11] S. Corson and J. Macker, "RFC 2501 Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," 1999.

[12] J. Hubaux, L. Buttyán, and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," *Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking & Computing*, 2001.

[13] M. Jahnke and J. Tölle, "Bedrohungen gegen taktische mobile Adhoc-Netzwerke (MANETs)," FGAN/FKIE, Wachtberg, Germany, Tech. Rep., December 2005, appointed by the Federal Office for information management and information technology of the German Federal Armed Forces [in German].

[14] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, 2002.

[15] W. Yu, Y. Sun, and K. R. Liu, "HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks," *Proceedings of the 24th IEEE INFOCOM*, 2005.

[16] B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens, and C. Nita-Rotaru, "On the Survivability of Routing Protocols in Ad Hoc Wireless Networks," *Proceedings of the 1st IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks*, 2005.

[17] J. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks," *Proceedings of the 2nd IEEE International Workshop on Information Processing in Sensor Networks*, 2003.

[18] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and Secure Source Authentication for Multicast," *In Network and Distributed System Security Symposium*, pp. 35–46, February 2001.

[19] J. T. A. Perrig, R. Canetti and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *In IEEE Symposium on Security and Privacy*, pp. 56–73, May 2000.

[20] F. Kargl, S. Schlott, and P. Weber, "Sensors for Detection of Misbehaving Nodes in MANETs," *Praxis der Informationsverarbeitung und Kommunikation (PIK) 01/2005, K.G. Saur, Munich, Germany*, 2005.

[21] M. Jahnke, J. Tölle, M. Bussmann, and S. Henkel, "Components for Cooperative Intrusion Detection in Dynamic Coalition Environments," *Proceedings of NATO/RTO IST Symposium on Adaptive Defence in Unclassified Networks*, 2004.

[22] J. Tölle, M. Jahnke, N. gentschen Felde, and P. Martini, "Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System," *Proceedings of the 25th Military Communications Conference (MILCOM 2006)*, 2006.

[23] A. Wenzel, "Sensorik fr Intrusion-Detection-Systeme in mobilen Adhoc-Netzwerken," Master's thesis, Computer Science Dept., University of Applied Sciences, Cologne, Germany, 2006.

[24] S. McCanne and S. Floyd, "ns Network Simulator," 2006. [Online]. Available: http://www.isi.edu/nsnam/ns/

[25] University of Bonn, "Bonn Mobility and Networking Suite," 2006. [Online]. Available: http://www.cs.uni-bonn.de/IV/bomonet/

[26] C. Bettstetter and C. Wagner, "The spatial node distribution of the random waypoint mobility model," *Proceedings of the 1st German Workshop on Mobile Ad-Hoc Networks (WMAN)*, 2002.

[27] J. Yoon, M. Liu, and B. Noble, "Random Waypoint Considered Harmful," *Proceedings of 22nd IEEE Infocom*, 2003.