Electronic Communications of the EASST
Volume 37 (2011)

Workshops der wissenschaftlichen Konferenz Kommunikation in Verteilten Systemen 2011 (WowKiVS 2011)

Wormhole Detection using Topology Graph based Anomaly Detection (TOGBAD)

Elmar Gerhards-Padilla, Nils Aschenbruck and Peter Martini

12 pages

Guest Editors: Horst Hellbrück, Norbert Luttenberger, Volker Turau
Managing Editors: Tiziana Margaria, Julia Padberg, Gabriele Taentzer
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Wormhole Detection using Topology Graph based Anomaly Detection (TOGBAD)

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: Routing Attacks are a serious threat to communication in tactical MANETs. TOGBAD is a centralised approach, using topology graphs to detect such attacks. In this paper, we present TOGBAD's newly added wormhole detection capability. It is an adaptation of a wormhole detection method developed by Hu et al. This method is based on nodes' positions. We adapted it to the specific properties of tactical environments. Furthermore, we present simulation results which show TOGBAD's performance regarding the detection of wormhole attacks.

Keywords: tactical multi-hop networks, TOGBAD, wormhole detection

1 Introduction

In tactical environments (i.e. military or disaster response scenarios) sensitive data (e.g. soldier positions) is transmitted via insecure links. Additionally, 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. Tactical multi-hop networks possess a property that can be exploited for security purposes. In such scenarios, there 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.

In the following, we assume that cryptographic keys are available and in use. Thus, confidentiality, integrity, and authenticity of transmitted packets are provided by cryptographic means. 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. One way to detect insider attacks is to use intrusion detection, or to be more specific anomaly detection. TOGBAD [GAM10], 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 this paper, we enhance TOGBAD with wormhole detection capability. In detail, we present studies on attackers launching a wormhole attack and an evaluation of TOGBAD's wormhole 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 wormhole attacks and their detection in

distance-bounding	time-bounding	statistical	structure-based	direction-based
[CBH03]	[CKLJ08]	[BDV05]	[HKT09]	[HE04]
[HPJ03]	[EKF06]	[GMW+06]	[HCJ07]	
[LPM+05]	[HPJ03]	[SQL05]	[MGD07]	
[KG08]	[KBS05]		[LS10]	
[WBLW06]	[SLG+07]		[WL06]	
[XOL+07]	[WBLW06]			

Table 1: Overview of Wormhole Research

multi-hop networks (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 and then show our evaluation concerning the quality of our wormhole detector (sect. 5). Finally, we conclude the paper (sect. 6).

2 Routing Attacks

In wireless multi-hop networks (e.g. MANETs, Mesh networks), every node of the network can 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 forge 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. These attacks are already mentioned in previous work, e.g. in [HPJ03]. In this paper we focus on an attack known as wormhole attack.

To launch a wormhole attack, one or more attackers capture traffic in one region and replay it in a distant region of the network. There are different ways to realize such a wormhole. They can be classified into in-band or out-of-band wormholes. This classification is based on the channel used by the attackers. If the attackers use the channel of the attacked network, it is named an in-band wormhole. Consequently, if the attackers use a separate channel for communication, it is named an out-of-band wormhole. In this paper, we focus on an out-of-band wormhole, since an in-band wormhole has two major drawbacks. First, the route to the destination node may fall prey to the attack itself and no route may be found. Second, the in-band wormhole introduces a significant delay. Therefore, one may question the impact such an attack would have. For details on different possibilities to launch a wormhole attack we refer to [KBS05]. In the following, we consider two collaborating attackers using an out-of-band link to tunnel traffic.

3 Related Work

The research conducted concerning wormhole attacks in multi-hop networks so far can be divided into five categories (cf. Tab. 1): distance-bounding, time-bounding, statistical, structure-based and direction-based. Distance-bounding approaches use geographical information to bound the distance between two nodes able to communicate with each other. Time-Bounding ap-

proaches introduce time restrictions (e.g. on answering to requests) to detect wormholes. Statistical approaches use statistical means for wormhole detection. Structure-based approaches observe the network structure and use special structures induced by wormholes for detection. Direction-based approaches use the direction a transmission is sent/received from for detection purposes.

[HE04] is a direction-based approach. It uses directional antennas. Each antenna is assigned different zones and determines for each message in which zone the received signal power is maximal. Neighboring nodes should receive each other's transmissions in opposing zones. This approach requires directional antennas and therefore can not be applied in all kinds of networks.

[HKT09], [HCJ07], [LS10], [MGD07] and [WL06] are structure-based approaches. [HKT09] introduces DeWorm, a protocol to detect wormhole attacks. Its basic idea is to compare the length of alternative routes not passing through the wormhole to the length of routes including the wormhole link. Due to the shortcut induced by a wormhole the alternative paths are significantly longer than the paths using the wormhole link. This approach requires feedback from the nodes on the route through the wormhole. Thus, it does not work for insider wormholes since an insider may give false feedback to disturb the wormhole detection. [HCJ07] identifies structures in the 2-hop neighborhood of sensors. Based on these information shortcuts induced by a wormhole are identified and virtual links are removed. Since not all shortcuts found by this approach result from wormholes, the approach is subject to false alarms. [LS10] analyses the neighborhood of nodes and detects anomalies in the connectivity information. The proposed protocol works under some assumptions. One is that the nodes are uniformly and densely distributed. This assumption is not valid for tactical multi-hop networks. Thus in these networks the protocol is not applicable. In [MGD07] each node locally checks if there are forbidden structures in its connectivity graph. This approach requires nodes to have detailed knowledge of the connectivity in their k-hop neighborhood with k potentially greater than 2. In highly dynamic environments like tactical multi-hop networks this knowledge is very hard to gain and maintain. [WL06] uses a combination of visual representation of network topology, user interaction, and automatic analyses to defend against wormholes. The network topology is visualized and based on the shortcuts induced by a wormhole the attack is detected. This approach requires user interaction and thus is not applicable to tactical environments with non-expert users potentially under high stress.

[BDV05], [GMW+06] and [SQL05] fall into the category of statistical approaches. [BDV05] is a wormhole detection approach for sensor networks. It uses statistical means to detect variances in number of neighbors or an increase in the number of short routes. The algorithms run on the base station in sensor networks. The approach assumes that sensor nodes securely can transmit valid neighborhood information to the base station. Thus, the base station has a central, correct view of the actual network topology. In more dynamic tactical multi-hop networks it is very difficult to gain such a precise view on the network topology. Especially to gain a view that is not influenced by the wormhole. [GMW+06] bases on timing analyses of routing traffic in a network. Proactive routing protocols need to exchange management information on a periodic basis. The assumption is that a wormhole leads to a significant delay and thus can be detected by timing analyses. The approach is only applicable with proactive routing protocols. [SQL05] considers an on-demand multi-path routing protocol. Wormholes are detected by checking the relative frequency a link appears in reply to one route discovery and the difference of appearances

between the most frequently appeared link in one response to second most frequently appeared link. The approach is restricted to on-demand protocols.

[CKLJ08], [EKF06], [KBS05], and [SLG+07] are time-bounding approaches. In [CKLJ08] nodes measure the time until a reply to a given request reaches the sender of the request. If this time exceeds a threshold, a wormhole is assumed. Depending on the type of wormhole, the reply via the wormhole can reach the sender of the request earlier than the reply via the valid route. Thus, this approach is not able to detect all kinds of wormholes. [EKF06] introduces TrueLink, a timing based countermeasure to wormhole attacks. Link verification is performed between neighboring nodes and is based on the assumption that a wormhole is not able to relay messages fast enough to break the strict timing constraints used in the link verification procedure. This approach does not work against attackers having compromised nodes and announcing links between themselves. [KBS05] uses guard nodes for links. Each guard node has a threshold on the time when a packet must be forwarded by the observed nodes. If this threshold is exceeded, the guard generates an alarm. For this approach, the guard nodes need to reliably overview all transmissions, which is not trivial in wireless networks. [SLG+07] considers only in-band-wormholes. The wormhole detection is based on the increased round-trip-time induced by in-band-wormholes. Since out-of band wormholes may even shorten round-trip-times, the detection method from [SLG+07] does not work against all kinds of wormholes.

[HPJ03] presents a distance-bounding as well as a time-bounding approach, while [WBLW06] combines distance and time-bounding. [HPJ03] introduces geographical and temporal packet leashes. For the geographical leash approach, each sending node includes its location and the sending time of the packet in each packet. Each node approximates the propagation ranges. Based on its approximation and the information in the packet concerning position of the sending node and sending time of the packet, a receiving node may check whether the packet travelled a distance above the maximum transmission range of a benign node. For the temporal leash approach, each sending node includes the sending time of the packet in each packet. Each receiving node determines if the packet traveled too far based on the reception and sending time of the packet, the speed of light, and maximum transmission range of a benign node. Using these approaches each node, including the light-weight nodes in tactical environments, checks packets for plausibility. This leads to calculation effort for each node which shortens the lifetime of the light-weight nodes. [WBLW06] is an end-to-end approach. For detection of false packets, the sending node includes the sending time and its position in the packet. Each intermediate node attaches time and position when it receives and forwards the packet to the packet. Based on these informations plausibility checks are performed concerning claimed neighborhood, moving speed of nodes, and traveling time of the packet. Data, routing, or separate packets may be used as detection packets. By using this approach the major part of the calculations (e.g. the plausibility checks) has to be done by the receivers. As lightweight nodes are receivers as well, this approach may not be usable.

[CBH03], [KG08], [LPM+05] and [XOL+07] use distance-bounding approaches. [CBH03] proposes Mutual Authentication with Distance-Bounding (MAD). It uses a challenge-response technique to determine an upper bound on the physical distance between nodes. Thus, a node cannot cheat another node by appearing to be closer than it really is. [KG08] performs a test on end-to-end basis. Detection packets are used where each node transmitting such a packet attaches its location and range to the packet. Routing, data, or separate packets may be used as

detection packets. The destination node checks whether the distance travelled by the packets is plausible given the hop count of the packet. If the travelled distance is not plausible, a wormhole is detected. Again, this approach may lead to high effort for the light-weight nodes in tactical environments. [LPM+05] uses guard nodes. The detection of a wormhole is based on the single guard property (reception of multiple copies of an identical message from one guard) and the communication range constraint property (a node hears two guards which are too far apart). [XOL+07] first creates a representation of the network using probe packets which are flooded through the network. Based on the information gained in this step, each node computes a local map for its neighbors. If the maximum distance between two neighbors of one node in such a local map exceeds a certain threshold, a wormhole is detected.

To the best of our knowledge, our approach is the only one especially tailored to the specific characteristics of tactical environments. By using information available in such environments, we are able to use synergies and reduce the overhead induced by our approach. Furthermore, the detection routines run on the fully equipped nodes. This minimizes the effort for the light-weight nodes sparing critical resources like energy and CPU power.

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. A detailed description of a preliminary version can be found in [GAM10].

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 this, the detection instances are able to detect nodes propagating fake topology. However, without enhancements this version of TOGBAD is not able to recognize wormhole attacks. For more details to the basic functioning of TOGBAD we refer to [GAM10].

4.2 Wormhole Detector

The basic idea of the wormhole detector is the one of the geographical leashes approach introduced in [HPJ03]. The distance travelled by packets in the network is checked for plausibility. In the following, we present our approach TOGBAD-Wormhole which is an adapted version of the geographical leaches approach.

Our approach uses a period-based detection method. The sensor instances of TOGBAD send reports about received packets to the detection instances of TOGBAD. At the detection instances, for every reported link the distance a packet travelled over this link is checked. These link-based detections are aggregated to a period-based detection.

The method takes advantage of the topology graph created by TOGBAD. This topology graph offers a global view on the network topology. Additionally, each node in the graph is associated with its node position. This enables TOGBAD-Wormhole to check the reported links in the network for plausibility. A single-link based approach is prone to detection errors. A single link might be falsely classified for a number of reasons, e.g. due to position inaccuracies. Therefore, we use a period-based approach. In a given time frame, our approach aggregates the single decisions and decides based on this aggregation whether an attack occured or not. This detection method takes advantage of a wormhole attack's special property in wireless networks.

When a wormhole attacker is able to capture and replay a packet from one node, at the end of the wormhole tunnel the packet is usually not only received by a single node, but rather a larger number of nodes. Hence, the period-based detection method analyzes all links reported in the last period. It triggers an alarm, if at least k links -with the same link's source node- are detected as wormhole links during a detection period. In this work, we manually choose a static threshold k. In an ideal world the optimal threshold would be the number of nodes that receive the replayed packets of a wormhole attacker. However, in reality one cannot determine this number. Thus, the choice for the threshold should be based on the number of neighbors for each node, since this gives an approximation of the number of reports to be expected over a node's behavior. At this point it is left as future work to determine the threshold automatically and dynamically. In Detail, TOGBAD-Wormhole works in the following way: Let be pos_A the position of node A, t the current time, U_A the time of the last position update of node A, v the maximum velocity of a node and δ the maximum position error then: $dist(A,B) := \|pos_A - pos_B\| - (2*t - U_A - U_B)*v - 2*\delta$.

Let be CR_A the maximum communication range of node A. The detection instances consider a link malicious, if $dist(A,B) > CR_A$.

This is the already mentioned link-based detection, which is an only slightly changed variant of the geographical leashes approach by Hu et al. [HPJ03]. In our period-based approach, the detection instances generate an alarm, if #malicious links $>$ threshold k.

Compared to the geographical packet leashes approach from [HPJ03], the three main differences of our approach TOGBAD-Wormhole are: (a) Central plausibility check. In our approach the check of the distance is not done at every node but centrally at the detection instances. This spares critical resources at the light-weight nodes. (b) Aggregation of detections. An alarm decision on a per packet basis may lead to a high number of false alarms. Therefore, we aggregate single detections and decide on a periodical basis whether a wormhole is present or not. (c) No alteration of data/routing packets necessary. Our approach does not need the addition of information to data/routing packets. In tactical environments there is a command & control system present and therefore at the fully equipped nodes node positions are available. Thus, we use synergy effects to minimize the overhead of our approach.

5 Evaluation

To evaluate our approach, we conducted simulations. In this section, we first introduce the used simulation environment and afterwards present our simulation results. Concerning our simulation results, we first investigate the detection rate of a link-based approach (5.1). Afterwards, we show the detection rate of our new, period-based approach (5.2) with and without packet loss.

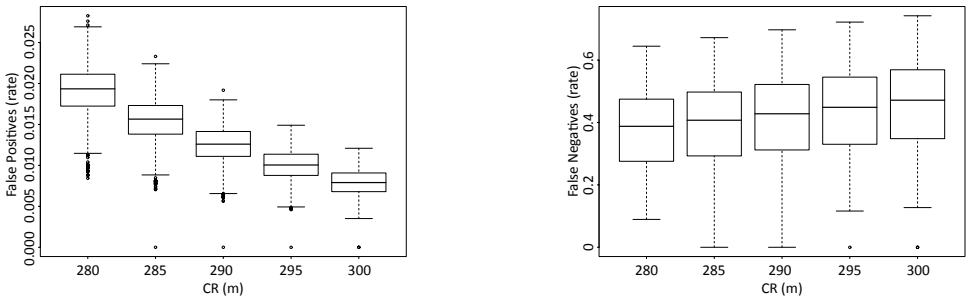
Since we consider tactical environments, we choose Reference Point Group Mobility (RPGM) [HGPC99] as mobility model. Due to the general characteristic of the wormhole attack only routes with two or more hops are typically affected by the attack, when considering hop-count based routing protocols. However, RPGM scenarios offer only a limited number of multi-hop routes due to the properties of the applied RPGM mobility model. Nevertheless, in tactical scenarios there typically are two kinds of communication channels present, intra-group and inter-group. In the following the inter-group communication channel is depicted as command channel. Typically, the communication between tactical command and the troops in the field is inter-group and therefore multi-hop communication. Thus, it is important to not only consider one-hop but also multi-hop routes. Hence, 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 for voice communication that is attacked by a wormhole in the conducted simulations. Due to the high amount of group-based communication in tactical scenarios, we use multicast traffic for the voice communication. All nodes are equipped with radio hardware with a maximum communication range of approximately 300m. All packets are sent with a transfer rate of 11Mbps and are routed by applying the Simplified Multicast Forwarding (SMF) protocol using S-MPR (cf. [Mac09]). A combination of log-distance and ricean fading is used as signal propagation model. The modelled military mission consists of several fireteams of infantry soldiers that are moving in an area of 1000m x 1000m. Each RPGM group consists of 5 nodes, which approximates the size of a military fireteam. The maximum distance between a unit and its corresponding group center is set to 300m to model a closely operating infantry squad.

Since voice traffic is one of the main applications in tactical networks, we consider voice traffic at 2400bps according to the specification of the MELP-Codec (Mixed-Excitation Linear Predictive Coder, cf. [NAT02]). To create this traffic, we use the traffic model for disaster area scenarios introduced in [AGFM06]. Each node is member of one global talk group to model inter-group communication. Beside that, each modeled military squad has a local talk group, i.e. each node is also member of a local talk group to model intra-group communication.

Node numbers of 15, 30 and 45 are considered. The scenarios' node density increases by the number of nodes, because all nodes are distributed on an area of equal size. For each node number 400 replications are done with varying movements and traffic for a duration of 500 seconds. Additionally, only replications with a non-partitioned network for at least 90% of the simulation time are considered, in order to prevent that two partitions are only connected over a wormhole link, which will inevitably attract much traffic and may then distort simulation results.

Since the attackers will try to maximize their impact, they most likely will not attack nodes in the same local talk group. Thus, in the RPGM scenarios, we uniformly choose the attackers from different groups. Each attacker captures as much traffic (data and routing packets) as possible (i.e. acts in promiscuous mode) and tunnels the captured traffic to the colluding attacker via an



(a) link-based, FP (b) link-based, FN

Figure 1: False Positives, False Negatives link-based approach

out-of-band link. Finally, the colluding attacker replays the tunneled traffic. The attackers tunnel traffic between seconds 100 and 500 in all scenarios.

5.1 Link-based Approach

To demonstrate the benefit of our period-based approach, we first show results gained with a link-based approach without aggregation of single detections. As metrics we use the rate of False Positives and False Negatives.

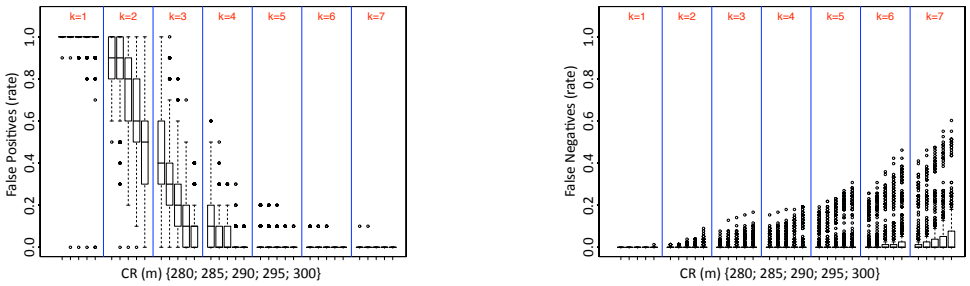
Fig. 1(a) shows the rate of False Positives for different choices of the threshold for the maximum communication range (CR) of a node. In this figure the threshold is chosen between 280 and 300 meters. For all thresholds in this interval the median of False Positives is below 2%. The median of False Positives decreases with increasing threshold down to below 1%. Due to the increasing threshold a greater distance for each link is considered valid. Thus, less links are considered malicious and the number of False Positives decreases.

In Fig. 1(b) the rate of False Negatives for different thresholds CR are shown. The rate of False Negatives is significantly greater than the rate of False Positives. Even for a threshold of 280m the median is at approximately 40%. It further increases with increasing threshold. Thus, the number of False Negatives is way to high for the link-based approach to work properly in a realistic environment. The reason for the increase of the False Negatives with increase of the threshold is analog to the explanation for Fig. 1(a). With increase of the threshold less links are considered malicious. Thus, the number of False Negatives increases.

5.2 Period-based Approach

In this section we evaluate our new period-based approach. As metrics we use again the rate of False Positives and False Negatives. We first show the performance of our approach for different choices of CR and k. Afterwards, we show the impact of packet losses on the detection rate for one specific choice of CR and k.

The period-based approach analyses all links it is aware of, aggregates these analyses and



(a) period-based, FP

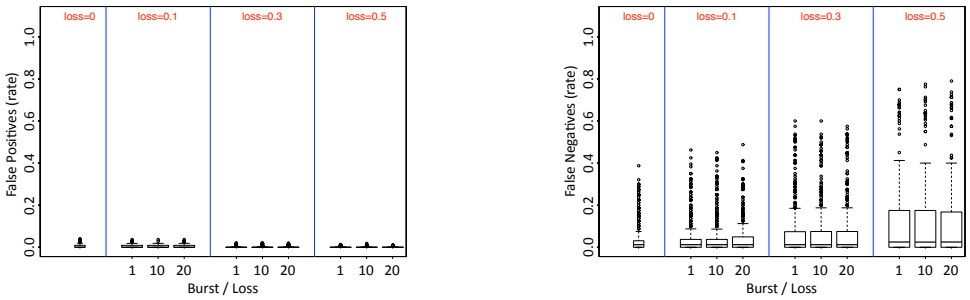
(b) period-based, FN

Figure 2: False Positives, False Negatives period-based approach

generates an alarm if the number of detected wormhole links exceeds a threshold k. The performance of the period-based approach heavily depends on the choice of the threshold k. Therefore, in the following we pick the threshold k from the set $\{1;2;3;4;5;6;7\}$ to adequately vary k. Additionally, we vary CR again between 280m and 300m, like we did for the link-based approach (cf. Fig. 1). Fig. 2(a) illustrates the rate of False Positives over different choices of k and CR. Independent on the choice of CR, for k = 1 the median of False Positives stays at 100%. With increasing k and CR the rate of False Positives decreases. In particular greater choices of k lead to a significant decrease of False Positives. For a choice of k = 4 (in combination with an appropriate CR) the median of False Positives drops to 0%. For $k > 4$ the median of False Positives stays at 0% independent on the choice of CR.

Fig. 2(b) shows the rate of False Negatives over different choices of k and CR. The median of False Negatives stays at 0% for all choices of CR and k. The number of outliers increases with increasing k. For k = 6 and k = 7 the upper quartile also increases. For small choices of k the detector generates an alarm for almost every round. This leads to an extremly high number of False Positives and nearly no False Negatives. Nevertheless, with reasonable combinations of k and CR the period-based detector leads to very good results with the median of False Positives and False Negatives both at 0%. Especially a choice of k = 4 and CR = 300 leads to low False Positive and False Negative rates. Therefore, in the following we use k = 4 and CR = 300. Altogether, by aggregating the single analyses the detection rate is significantly improved compared to the link-based approach.

Our approach relies on reports sent from the sensor instances to the detection instances. Hence, it is important to evaluate which impact losses of these reports have on the performance of our approach. Thus, we consider the same scenarios as in the previous evaluation, but this time we consider bursty packet losses. To model packet losses, we use a two-state Markov chain with states loss and no loss. We vary packet loss rate and average burst length to measure both the impact of increasing loss rate and burst length. Fig. 3(a) shows the rate of False Positives over different packet losses and burst lengths. The median of False Positives does not increase with increasing burst length or increasing packet loss. For increasing packet loss the upper quartile



(a) FP with packet loss

(b) FN with packet loss

Figure 3: False Positives, False Negatives period-based approach with packet loss

even decreases. If the number of reports reaching the detection instances decreases, the number of links considered malicious decreases. This leads to a decreased number of alarms and in consequence to fewer False Positives.

Fig. 3(b) illustrates the rate of False Negatives over different packet losses and burst lengths. The median of False Negatives does not increase for increasing burst length, but slightly increases for increasing packet loss up to around 5% for a packet loss of 50%. The reason is again the lesser number of reports reaching the detection instances. Thus, the number of reported malicious links is smaller compared to the situation without packet losses and the number of False Negatives increases. However, the approach is very robust against packet losses. Even for heavy packet losses and long loss bursts, the median of False Positives and False Negatives stay very low with 0% respectively 5%.

In total, the period-based approach yields very low rates of False Positives and False Negatives and thus a very good detection of wormhole attacks. Especially the aggregation of single analyses significantly improves the detection rate. Additionally, the approach is very robust against packet loss. Critical for the approach is the choice of the threshold k. One approach could be to adapt the threshold dynamically. This is beyond the scope of this paper and left for future work.

6 Conclusion and Future Work

In this paper we introduced a new wormhole detection capability to our intrusion detection approach TOGBAD. We adapted an existing approach by Hu et al. to tactical environments and modified it to work in a period-based manner. By doing so, we significantly improved its detection rate concerning a wormhole attack. Our approach is a centralistic distance-bounding one. At the detection instances the distance of each link is checked for plausibility. The single analyses are aggregated. If a number of links above a certain threshold are considered as malicious, an alarm is generated. With our modifications the approach showed a very low False Positive and False Negative rate. It reliably detected the considered wormhole, even under heavy packet losses. However, there are still questions which have to be examined in the future. Our approach

has to be tested in more realistic scenarios concerning the mobility model. Furthermore, a reasonable choice for the threshold k has to be evaluated. Finally, a method to automatically and dynamically determine the threshold should be developed.

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

Bibliography

[AGFM06] N. Aschenbruck, M. Gerharz, M. Frank, P. Martini. Modelling Voice Communication in Disaster Area Scenarios. *Proc. of LCN*, 2006.

[BDV05] L. Buttyán, L. Dora, I. Vajda. Statistical Wormhole Detection in Sensor Networks. In *Security and Privacy in Ad-hoc and Sensor Networks*. 2005.

[CBH03] S. Capkun, L. Buttyán, J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proc. of SASN*. 2003.

[CKLJ08] S. Choi, D. young Kim, D. hyeon Lee, J. il Jung. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks. In *Proc. of SUTC*. 2008.

[EKF06] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos. TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks. In *Proc. of ICNP*. 2006.

[GAM10] E. Gerhards-Padilla, N. Aschenbruck, P. Martini. TOGBAD - An Approach to Detect Routing Attacks in Tactical Environments. *accepted for Wiley Security and Communication Networks*, 2010.

[GMW+06] M. Gorlatova, P. Mason, M. Wang, L. Lamont, R. Liscano. Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis. In *Proc. of MILCOM*. 2006.

[HCJ07] Y.-T. Hou, C.-M. Chen, B. Jeng. Distributed Detection of Wormholes and Critical Links in Wireless Sensor Networks. In *Proc. of IIHMSP*. 2007.

[HE04] L. Hu, D. Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Proc. of NDSS*. 2004.

[HGPC99] X. Hong, M. Gerla, G. Pei, C. Chiang. A group mobility model for ad hoc wireless networks. *Proceedings of ACM International Workshop on Modeling, Ana- lysis and Simulation of Wireless and Mobile Systems*, 1999.

[HKT09] T. Hayajneh, P. Krishnamurthy, D. Tipper. DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks. In *Proc. of NSS*. 2009.

[HPJ03] Y.-C. Hu, A. Perrig, D. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proc. of INFOCOM*. 2003.

[KBS05] I. Khalil, S. Bagchi, N. B. Shroff. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks. In *Proc. of DSN*. 2005.

[KG08] S. Khurana, N. Gupta. FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks. In *Proc. of SECURWARE*. 2008.

[LPM+05] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. Chang. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *Proc. of WCNC*. 2005.

[LS10] C. Lee, J. Suzuki. *SWAT: A Decentralized Self-healing Mechanism for Wormhole Attacks in Wireless Sensor Networks*. Handbook on Sensor Networks. World Scientific Publishing, 2010. ISBN: 978-981-283-730-1.

[Mac09] J. Macker. IETF Draft Simplified Multicast Forwarding for MANET. *http://www.ietf.org*, 2009.

[MGD07] R. Maheshwari, J. Gao, S. R. Das. Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In *Proc. of INFOCOM*. 2007.

[NAT02] NATO Standardization Agency. The 1200 and 2400 Bit/s NATO Interoperable Narrowband Voice Coder. *STANAG 4591*, 2002.

[SLG+07] D. Sterne, G. Lawler, R. Gopaul, B. Rivera, K. Marcus, P. Kruus. Countering False Accusations and Collusion in the Detection of In-Band Wormholes. In *Proc. of ACSAC*. 2007.

[SQL05] N. Song, L. Qian, X. Li. Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach. In *Proc. of IPDPS*. 2005.

[WBLW06] W. Wang, B. Bhargava, Y. Lu, X. Wu. Defending against Wormhole Attacks in Mobile Ad Hoc Networks. In *Wireless Communications and Mobile Computing*. January 2006.

[WL06] W. Wang, A. Lu. Interactive Wormhole Detection in Large Scale Wireless Networks. In *Proc. of VAST*. 2006.

[XOL+07] Y. Xu, Y. Ouyang, Z. Le, J. Ford, F. Makedon. Analysis of Range-Free Anchor-Free Localization in a WSN under Wormhole Attack. In *Proc. of MSWiM*. 2007.