Intrusion Detection in Tactical Multi-Hop Networks

Elmar Gerhards-Padilla
University of Bonn - Institute of Computer Science IV
Roemerstr. 164, 53117 Bonn, Germany
padilla@cs.uni-bonn.de

Marko Jahnke, Alexander Wenzel
FGAN - FKIE
Neuenahrer Str. 20, 53343 Wachtberg, Germany
{jahnke, wenzel}@fgan.de

I. Introduction

Multi-hop networks such as Mobile Ad hoc NETworks (MANETs) are an emerging technology which shows great promise especially in tactical scenarios where no fixed infrastructure is available. Due to the collaborative nature of the employed algorithms (e. g. routing) and the open medium, tactical multi-hop networks are particularly susceptible to attacks. Thus, an appropriate monitoring system is required which is capable of reliably detecting different kinds of attacks. In two research projects called MITE (MANET Intrusion Detection for Tactical Environments) and RITA, funded by the German armed forces, a distributed intrusion detection system (IDS) for tactical MANETs has been developed. An overview of the system can be found in [9]. In the following, this IDS is called RITA IDS.

In typical scenarios like infantry deployment there are different kinds of nodes. On the one hand there are lightweight nodes—handheld communication devices of soldiers. On the other hand there are fully equipped nodes—larger communication devices that are integrated into troop carrier vehicles and have access to a larger power supply. The developed IDS uses the fully equipped nodes for centralized IDS approaches, while the lightweight nodes, beside running some resource-efficient sensors, can act as watchdogs. Figure 2 provides an architectural overview of the system. Several new intrusion detection sensors and detectors were developed and integrated into the RITA IDS. Furthermore, different existing approaches were adapted and integrated as well. Section II provides an overview of the different approaches integrated into the system.

Our prototypical implementation has been successfully evaluated with different numbers of real-world nodes as well as extended by emulation of virtual MANET nodes (cf. [8]). For the evaluation, an example scenario consisting of a hostage rescue infantry deployment is considered. In the scenario, 15–20 soldiers are equipped with wireless-enabled handheld devices (see fig. 1). The scenario is characterized by a scenario-based motion and traffic sequence which is specific to the infantry deployment and more realistic than the commonly used mobility models.

II. Detection Approaches

This section provides an overview of the different detection approaches integrated into the IDS.

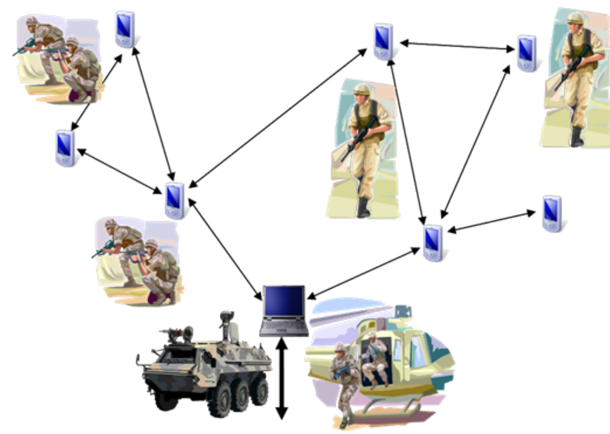

Fig. 1. Reference Scenario

A. Detecting Attacks against Routing

Since a MANET does not have a fixed infrastructure, communication is dependent on ad hoc routing and multi-hop packet forwarding. The collaborative routing protocol ensures resilient IP-layer connectivity and efficient packet delivery based on selected routing metrics. Attacks against this protocol might lead to service disruption, eavesdropping, and other unforeseeable adverse effects (e. g. routing loops). This could potentially result in significant tactical disadvantages. Detection of attacks against MANET routing is performed on a centralized as well as a local level. On the one hand, the topology graph-based anomaly detection (TOGBAD, [5], [4]) is used on the fully equipped node. A global topology graph of the entire network is created centrally, based on sniffed data and control packets that were transmitted in the network. For each node, the number of its neighbors is extracted from the topology graph and compared to the number of neighbors advertised in routing messages. Inconsistencies are reported to the RITA console. On the other hand, a local routing detector (LRD) on the lightweight nodes performs plausibility checks for each routing message. The approaches realized for the LRD are similar to those in [11] and [2].

B. Detecting Attacks against Packet Forwarding

Detection of packet drop attacks is accomplished locally on every node by an extended watchdog application. When a packet is sent (or relayed) to a neighbor node, the sending node waits until it senses that the packet has been retransmitted

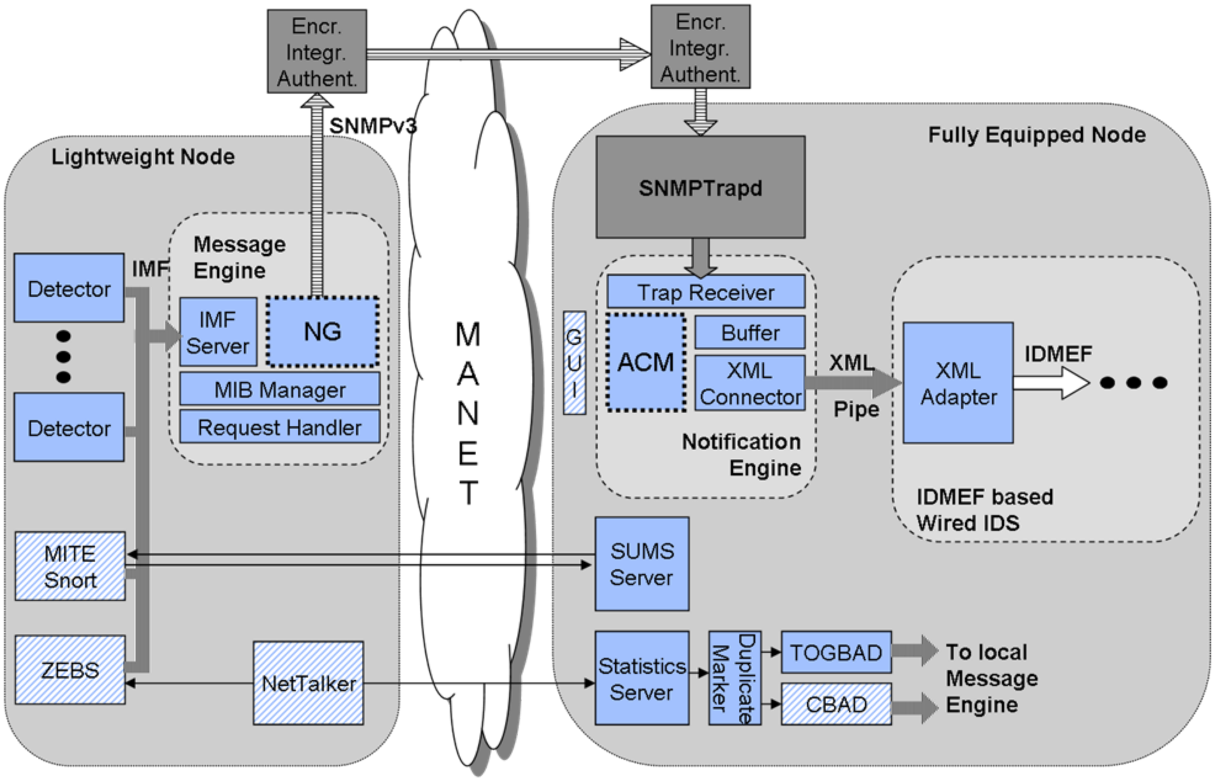

Fig. 2. IDS architecture with client and server components

by the relay node. Due to the symmetric propagation of radio waves in all directions, this is usually possible. Signal fading, medium collisions, devices' power-saving modes, and other adverse effects on packet relay are taken into account, and alerts are triggered accordingly if packet retransmission does not take place within a specific time frame.

C. Detecting Attacks against IP Networking

Like every IP-based network, MANETs are also vulnerable to traditional attacks on and above the IP layer, such as header modification, illegal protocol states, or malicious payloads. These attacks are often preceded by port scans or other abnormal activities. In our previous work we developed a cluster-based anomaly detector (CBAD, [3]) that is capable of recognizing IP-layer attacks by performing round-based distributed traffic structure analysis. In the RITA IDS we integrated a MANET-specific adaption of CBAD. For the integration of existing signature-based intrusion detection solutions (e. g. Snort$^{\text{TM}}$, [10]), the signature update management system (SUMS) is responsible for the resource-efficient distribution of signature updates through the entire MANET. This is achieved by a robust distribution protocol capable of differential updates.

D. Supporting Components and Open IDS Sensor-Detector Infrastructure

The open and highly extensible IDS infrastructure (see fig. 2 and [7]) allows the integration of arbitrary sensors

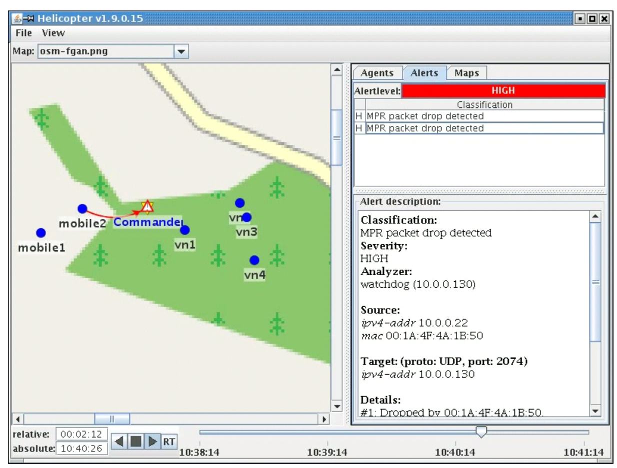

Fig. 3. Graphical user interface visualizing IDS events and node status

and detectors that are deployed on every MANET node. Sensors monitor relevant network areas and may be queried by detectors. IDS components save their current state in an SNMP MIB. Detectors send SNMP notifications to a RITA console in a standardized format (IDMEF, [1]). Event messages can be fed into a higher-level IDS (meta-IDS). Resource-efficient sensor/detector implementations (e. g. [6]) accommodate the reduced computing power of mobile nodes.

III. DEMO

Our demonstrator environment currently consists of three Internet Tablets representing the infantrymen's devices (lightweight nodes), several virtual nodes, and a more powerful laptop computer (fully equipped node). On the lightweight nodes, the RITA IDS transparently monitors the relevant parameters in the background, whereas the fully equipped node hosts the IDS console application (see fig. 3) to which all alerts are transmitted.

The goal of the demo is to demonstrate the RITA IDS. Thus, we will show a live demo by launching different attacks in our testbed. Depending on the kind of attack, several different detectors will send SNMP notifications to the IDS console. By doing so we will also present our combined evaluation testbed.

Further details concerning the demo:

Equipment:	2 laptops and 3 Internet Tablets
Space:	table and space for 2–3 posters
Setup time:	approx. 1 h
Additional facilities:	power supply
	video-projector or large TFT

ACKNOWLEDGEMENT

Parts of this work have been sponsored by the Federal Office for information management and information technology of the German Federal Armed Forces (ITAmtBW). The authors would like to thank the RITA cooperation team for the sustainable discussions and work.

REFERENCES

[1] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)," IETF RFC 4765, 2007.

[2] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs," *Proceedings of the intern. Conference on Wireless Communications and Mobile Computing*, 2006.

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

[4] E. Gerhards-Padilla, N. Aschenbruck, and P. Martini, "Enhancements on and Evaluation of TOGBAD in Tactical MANETs," *Proceedings of the 27th Military Communications Conference (MILCOM)*, 2008.

[5] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tölle, "Detecting Blackhole Attacks in Tactical MANETs using Topology Graphs," *Proceedings of the 3rd LCN Workshop on Network Security*, 2007.

[6] J. Haag and S. Karsch, "Optimized Sensors for Intrusion Detection in Mobile Ad-Hoc Networks," *Proceedings of the Military Communications and Information Systems Conference*, 2007.

[7] M. Jahnke, S. Lettgen, J. Tölle, M. Bussmann, and W. U., "A Robust SNMP based Infrastructure for Intrusion Detection and Response in Tactical MANETs," *Proceedings of the GI/IEEE Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2006.

[8] M. Jahnke, J. Tölle, A. Finkenbrink, A. Wenzel, E. Gerhards-Padilla, N. Aschenbruck, and P. Martini, "Methodologies and Frameworks for Testing IDS in Adhoc Networks," *Proceedings of the 2nd ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet)*, 2007.

[9] M. Jahnke, A. Wenzel, G. Klein, N. Aschenbruck, E. Gerhards-Padilla, P. Ebinger, and S. Karsch, "MITE - MANET Intrusion Detection for Tactical Environments," *Proceedings of the RTO IST-22-PBM Symposium*, 2008, [Best Paper Award].

[10] Snort: Open Source Network Intrusion Prevention and Detection System, "http://snort.org/," 2008.

[11] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An Effective Intrusion Detection Approach for OLSR MANET Protocol," *Proceedings of the 1st Workshop on Secure Network Protocols (NPSec)*, 2005.