MITE – MANET Intrusion Detection for Tactical Environments[1]

Marko Jahnke, Alexander Wenzel, Gabriel Klein
Research Institute for Communication, Information Processing and Ergonomics
Neuenahrer Str. 20, 53343 Wachtberg
Germany

{jahnke, wenzel, g.klein}@fgan.de

Nils Aschenbruck, Elmar Gerhards-Padilla
University of Bonn
Institute for Computer Science IV
Römerstr. 164, 53127 Bonn
Germany

{aschenbruck, padilla}@fgan.de

Peter Ebinger
Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstraße 5, 64283 Darmstadt
Germany

peter.ebinger@igd.fraunhofer.de

Stefan Karsch
University of Applied Sciences Cologne
Institute for Computer Science
Steinmüllerallee 1, 51643 Gummersbach
Germany

karsch@inf.fh-koeln.de

ABSTRACT

Mobile ad hoc networks (MANETs) provide possibilities to realize IP-based networks without the presence of a fixed infrastructure. Therefore, this technology has also become attractive for tactical networks, such as in command posts, vehicle convoys, autonomous robot systems, and also for infantry troops. Due to its radio characteristics, it is widely known that MANETs may become subject to different kinds of attacks against their availability and against the integrity, authenticity, and confidentiality of the information that is transmitted, processed, and stored on their devices. In terms of information assurance, many protective measures need to be applied to these networks in order to make them deployable even for critical missions – in terms of intrusion prevention, detection, resistance, and response.

MITE (MANET Intrusion Detection for Tactical Environments) is a collaborative research project that aims at developing prototypical solutions for intrusion detection in MANETs – especially in tactical scenarios. Its results so far have been realized and evaluated as real-world implementations, with the emphasis on flexibility and demonstrability – not exclusively relying on simulation results. This contribution presents a broad overview of MITE, starting with the reference scenario and attacker model, continuing with the description of several detection approaches, a robust and resource saving sensor-detector infrastructure as well as supporting components and finishing with the discussion of evaluation results in terms of detection speed, preciseness and robustness. Additionally, future directions of the research project are explained.

1 INTRODUCTION

With the advent of mobile ad hoc networks (MANETs), IP-based networks with comparatively high bandwidths have become deployable as platforms for communication and information processing

[1] Published in: Proc. of the NATO/RTO Research Symposium on Information Assurance for Emerging and Future Military Systems (RSY IST-076), Ljubliana, Slovenia, Oct. 2008.

applications, even in the absence of fixed infrastructure. Thus, supporting networks with mobile nodes become increasingly attractive for supporting military scenarios, like command post networking, communication of vehicle convoys and autonomous robot systems, as well as for supporting infantry missions. Important information such as sensor data, equipment status information, and tactical orders may be reliably transferred to places where it is needed, in order to support the paradigm of Network Enabled Capabilities. The ability to handle multimedia data (e. g., voice, video) in these networks allows the efficient substitution of ancient technologies using highly interoperable IP-based networks and applications.

Like any other radio-based networking technology, MANETs are subject to different threats. These threats include outside attackers as well as misbehaving entities on the inside. Therefore, many different information assurance technologies need to be applied to protect these kinds of networks, such as data encryption, access control, identity management, and intrusion detection. Unfortunately, many of the well-established intrusion detection approaches and implementations are not immediately transferrable from infrastructure-based IP networks, since there are many extensive implications to the usage of radio links and the mobility of the respective devices. Not only has the attack surface for broadband and smart jamming been enlarged (exploiting protocol characteristics for saving energy or for becoming less detectable), but the danger of impersonation and MITM (man-in-the-middle) attacks in the network has also increased. The probability for false alarms and false accusations of nodes in the networks is significant due to the possibility of unsuccessful transfer of protocol packets. This possibility increases with physical motion in the network which leads to interruption of transmissions and fluctuation of routes. Additionally, there are no key locations in the network, where all relevant traffic may be observed and analyzed in order to detect malicious behavior, as was the case for routers, switches, and firewalls in wired IP networks.

MITE (MANET Intrusion Detection for Tactical Environments) is a collaborative research project, funded by the Federal Office of Information Management and Information Technology of the German armed forces (ITAmtBw). Its primary focus is on developing prototypical solutions for intrusion detection components which are suitable for tactical environments, especially for infantry missions, where the troops are equipped with highly mobile lightweight devices which are used as platform for tactical command & control information systems (C2IS), as well as for conventional voice and textual communication (VoIP, chat, e-mail). Different development, testing, evaluation, and demonstration environments have been set up, in which several sensors, detection modules, and supporting components communicate via a robust and resource-saving communication infrastructure.

The rest of this paper is organized as follows. Section 2 explains the infantry mission reference scenario and the technical requirements of the project. Section 3 presents different detection schemes for attacks against MANET routing and forwarding and theoretical results. Subsequently, detection methods for IP-layer attacks in MANETs are discussed in section 4. This is followed by a description of supporting components and the IDS infrastructure in section 5. Thereafter, evaluation results of the developed methods and tools are given in section 6.

2 REFERENCE SCENARIO AND DEMONSTRATOR ENVIRONMENT

This section briefly describes the military mission and the scenario in which a tactical MANET is deployed that is protected by the MITE IDS. The scenario has been used for further evaluation and demonstration activities as described later in this contribution.

Mission and Scenario

The military mission that was selected as the basis for the reference scenario is a hostage rescue (HR)

mission at a reasonably known location. The unit comprises 15–20 persons, and it arrives in an armored carrier vehicle at a location that is a few hundred meters away from the place where the hostage is held by the adversary. After leaving the vehicle, the infantrymen move towards the target location, occasionally leaving persons behind who act as rear guards (and additionally, as communication relays). When reaching an area from where there is a line-of-sight to the hostage, the infantrymen fan out, until a reasonable number of persons have reached positions for observing the target. Within a time period that may last up to one hour, the target and the adversary are closely observed, and the infantrymen try to optimize their positions with respect to a later assault (observation phase). Under nearly optimal conditions, the commander gives order to eliminate the adversary where needed, to quickly access the hostage, and to safely escort the hostage back to the carrier vehicle. Figure 1 illustrates the relative positions of the infantrymen during the observation phase.

Figure 1: Infantrymen's positions during the observation phase of the reference scenario

Considering a tactical MANET that supports this mission with communication and information services, we have the following assumptions: Each infantryman carries a highly portable mobile device (UMPC or PDA) that is connected to the MANET and is powered by a battery. Additionally, the unit commander is equipped with a laptop-like device that is also part of the MANET but has greater resources in terms of CPU, memory, and battery. We consider the commander as being located in the carrier vehicle and having additional access to a communication link to the command post.

A distributed command & control information system (C2IS) with instances on each of the MANET nodes supports the mission with up-to-date navigation information, tactical orders, and equipment status of own and blue forces. Sensor information is captured on many of the nodes and is transmitted to the commander's node in order to pass it to the command post for a common operational picture. Voice-based communication services – which are needed both for infantrymen's status reports as well as orders and tactical information from the commander – are also provided by the MANET nodes.

Attacker Model

A potential attacker against tactical MANETs has many possibilities to perform a variety of attacks against the tactical MANET. Beside broadband and smart radio jamming attacks, it is possible to eavesdrop on the traffic – which is therefore protected by appropriate cryptographic mechanisms. These attacks are very generic and not in the focus of our work.

We focus on insider attacks, i. e. attacks performed by legitimate participants of the network. Insider attackers are either saboteurs or adversary forces which have taken over a MANET node equipped with all necessary authentication and encryption material, such as keys, passphrases, or different types of tokens. Thus, an insider attacker of this type may take part in the routing and forwarding processes and is

therefore able to perform DoS attacks on different OSI layers (e. g. disruption of the link protocol or dropping of packets to be forwarded) as well as attacks on the MANET routing (e. g. forging of routing messages in order to attract more packets to facilitate cryptanalysis).

Testing, Evaluation, and Demonstration Environments

For testing purposes, we have built a setup that is as close to reality as possible, especially in terms of hardware and software that is used in the MANET. This decision was mainly driven by the fact that many research results published so far in the context of wireless networks are based on simulations, and that some of these were based on unrealistic assumptions or parameters. Thus, it was necessary to create a universal setup that can be used for evaluation as well as for demonstration purposes.

Besides using event-driven software simulations for examinations of certain details (e. g. evaluation of detection algorithms), we decided to create an emulation environment that is able to integrate a scalable number of mobile MANET hardware devices as well as virtual nodes. The former are used to support the demonstration, the latter for being able to analyze the network behavior with a larger number of nodes. We have developed a synchronous node motion evaluation framework called *MotionEmulator*. This framework is able to reproducibly change the connectivity between the MANET nodes on the IP layer, according to a mission-driven motion sequence, and a selectable radio wave propagation model. The changing geographic positions are simultaneously used as input for applications which rely on GPS data.

Using this framework, it was possible to deploy real hardware nodes (in our case, Ultra Mobile Personal Computers – UMPCs), running the Linux OS, as well as virtual nodes, realized as instances of the OpenVZ [20] virtualization environment. Using modified interface bridges of the OS kernel, it was possible for real and virtual nodes to communicate over the air. For creating the MANET testbed, a comparatively stable OLSR network with sufficiently high PDF (packet delivery fraction) for the reference motion sequence was established. On this network, we ran two reference applications: A multi-participant navigation system as an alternative to a not-yet-existent tactical C2IS, as well as VoIP communication applications in interactive and non-interactive modes.

Against these two reference applications, different attacks were implemented, so that the impact of the effect is not only measurable (e. g. in terms of low PDFs or packet delays), but also recognizable in the applications for demonstration purposes. For instance, progressively dropping packets of the VoIP stream is recognized as reduced speech quality, followed by interruptions, and finally the complete disruption of the audio stream.

3 DETECTING ATTACKS AGAINST OLSR ROUTING AND PACKET FORWARDING IN MANETS

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 local as well as a centralized level. On the one hand, the local routing detector (LRD) performs plausibility checks on received routing messages on each node. On the other hand, by using topology graph-based anomaly detection (TOGBAD), a global topology graph of the entire network is created centrally, based on sniffed data and control packets that were transmitted in the network. This is compared to the content of globally distributed routing messages. Detection of packet drop attacks is accomplished locally on every node by an extended watchdog

application that monitors the surrounding nodes for correct packet relay.

Local Rule-based Detection of Routing Attacks

The local detection of routing attacks is based on plausibility checks of received routing messages. Certain conditions must hold between routing messages (HELLO and TC) if they should represent a coherent view of the network topology. If one of these conditions is violated, this is an indication of a potential attack (cf. [7], [8]).

An attacker who tries to attack MANET routing (for example, a black hole or wormhole attacker) has to manipulate routing messages, generate new messages, or (selectively) reject legitimate routing messages. This misbehavior can be detected by the developed module. A black hole attacker may list a node in its TC message as neighbor that was not listed as a neighbor node in its preceding HELLO messages. In addition, a node can detect an attack if it is listed as a direct neighbor in a TC message by a remote node, e. g. a black hole attacker.

Node mobility and fluctuations in the radio range due to external influences lead to a dynamic network topology and (short term) changes in the routing tables. This must be taken into account to make sure that this behavior does not lead to a large number of false positives. Some tolerance must be built in for certain properties that compensate for the loss of individual routing messages, e. g. caused by radio interference.

A suitable language was needed that allows the formulation of conditions and dependencies between routing messages to detect potential attacks. State-based and event-based description languages are the most promising approaches for intrusion detection in MANETs. The state-based approach provides means for optimization, but no intuitive way for abstraction and modularization. In contrast to that, the event-based approach primarily provides an intuitive description of attack scenarios and possibilities for the abstraction and modularization. However, there are little means for optimization and no support for concurrency. Therefore, a new language was developed which combines both approaches (state-based and event-based) and fulfils the requirements of MANETs.

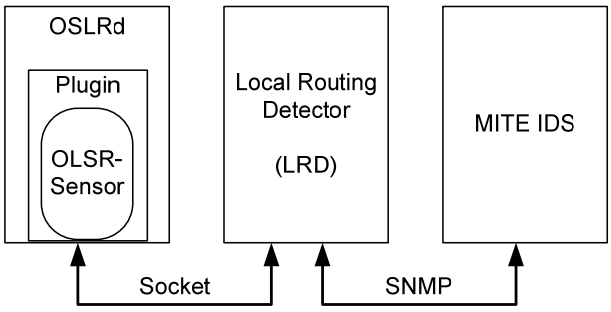

Figure 1: Integration of OLSR sensor and detector for local consistency checks of routing messages (LRD)

The module for local rule-based detection of routing attacks was implemented in the demonstrator environment. It is divided into two parts: an OLSR sensor for data collection and a detector for local consistency checks (local routing detector, LRD). The OLSR sensor was implemented as an OLSRd plug-in, which allows direct access to all parts of the OLSRd (see figure 1). The LRD was integrated with the OLSR sensor using a socket connection to allow local consistency checks of routing messages. The goal of the module is the identification of nodes that do not behave in a protocol-conformant way in an OLSR-based MANET.

Centralized Detection of Routing Attacks using Topology Graphs

In this section we present our approach for centralized detection of routing attacks called Topology Graph-based Anomaly Detection (TOGBAD). TOGBAD is a centralized anomaly detection method for routing attacks in tactical MANETs. It uses the structure of tactical MANETs by running the detection routines centrally on the fully-equipped nodes. It was first introduced in [1].

TOGBAD utilizes two types of instances corresponding to the two types of nodes present in tactical MANETs. The sensor instances of TOGBAD run on the lightweight nodes of the tactical MANET. These nodes act as watchdogs and periodically send reports to a detection instance. In these reports, the nodes include two types of information:

- Traffic flow information: Information from which nodes the sensor node has received traffic since the last report.
- Routing report: Information about the originator of and propagated number of neighbors from received routing messages.

The detection instances run on the fully-equipped nodes of the MANET. They receive and handle the reports of the sensor instances and are responsible for TOGBAD's detection process. The detection instances aggregate the information from the received reports and construct a topology graph that models the actual topology in the network. By sending fake routing messages, an attacker propagates a fake topology. The detection instances test the topology propagated by the nodes in the network against the actual topology represented in the topology graph. By doing so the detection instances are able to identify nodes propagating fake topology information.

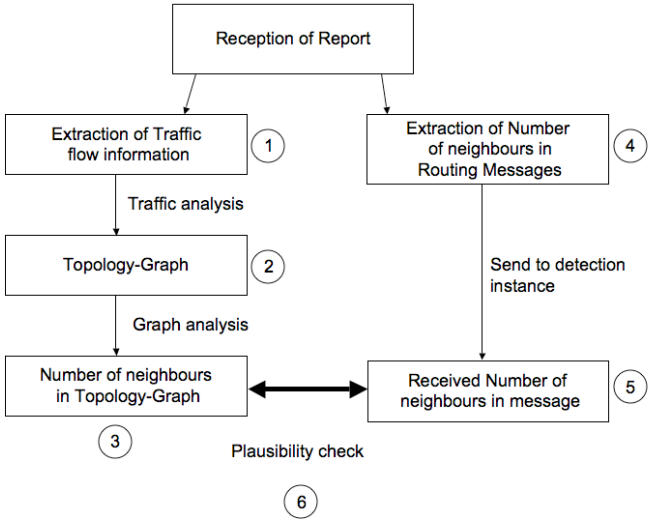

Figure 2: Functioning of TOGBAD

On reception of a report from a sensor instance, the detection process of TOGBAD consists of three parts.

1. First, the propagated number of neighbors is extracted from the report (figure 2, steps 4, 5).
2. Second, based on the traffic flow information in the received report, a topology graph is created or the existing graph is updated (figure 2, steps 1–3).
3. Finally, TOGBAD performs a plausibility check between the propagated number of neighbors and

the number of neighbors according to the topology graph (figure 2, step 6).

For more details on the basic functionality of TOGBAD, we refer to [1]. The differences (diff values) between the number of neighbors propagated by a node and the number of neighbors of the node extracted from the topology graph are defined as follows:

Let *o* be the originator of a routing message, *t(o)* the correct number of neighbors for *o*, *m(o)* the number of neighbors propagated in the routing message, and δ the deviation due to inaccuracies of the topology graph (e. g. due to node movement). Then,

$$diff := m(o) + \delta - t(o).$$

An alarm shall be generated if

$$diff > threshold.$$

The threshold is calculated by statistical analysis using empiric mean and estimated standard deviation. For each routing report that does not result in an alarm, we update mean, standard deviation, and threshold. In the following, x_i denotes the value of x calculated from the i-th routing report. For example, $threshold_3$ denotes the threshold calculated after reception of the third routing report.

For each node, we calculate a separate threshold in the following way:

We estimate the mean μ_i and standard deviation σ_i:

$$\mu_i = \mu_{i-1} + \alpha\,(diff_i - \mu_{i-1})$$

$$\sigma_i = \sigma_{i-1} + \beta\,(|diff_i - \mu_{i-1}| - \sigma_{i-1}).$$

The threshold is then calculated as

$$threshold_i := \max(1, \lceil \mu_{i-1} + w\,\sigma_{i-1} \rceil).$$

Enhanced Watchdog

Packet drop attacks in multi-hop networks can be detected using so-called *watchdog* or *overhearing* methods. Selective or entirely non-discriminate packet drops are often part of black hole attacks in MANETS (cf. sect. 2, [18]). Detection is based on the assumption that with symmetrical radio propagation, packets sent (or relayed) to a neighbor node have to be received over the air again when the neighbor in turn relays the packet.

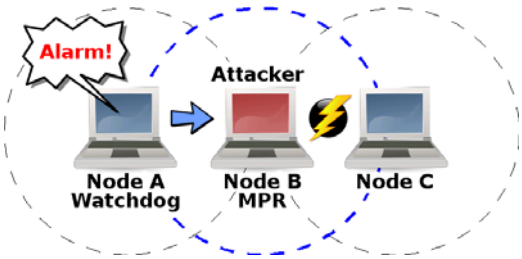

Figure 3: Functionality of watchdog for smart package drop detection

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 saves the packet's important properties and compares them to those of packet retransmitted by the relay node (cf. figure 3). Because radio waves propagate in all directions, this packet reception is usually possible. If, within an appropriate time frame, reception of a packet matching the saved properties does not occur, the packet is assumed to have been dropped. An alert is generated if a certain threshold is exceeded. This threshold needs to be set in accordance with potential adverse effects on packet relay, such as signal fading, medium collisions, or devices' power-saving modes.

4 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. A MANET-specific cluster-based anomaly detector (CBAD) is capable of recognizing IP-layer attacks by performing round-based distributed traffic structure analysis.

For the integration of existing signature-based intrusion detection solutions (e. g. Snort™), 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.

Cluster-Based Anomaly Detection (CBAD)

CBAD detects attacks that lead to changes in the structure of the observed traffic. These can, for example, be denial-of-service attacks or worms. The basic idea of CBAD is to model the structure of "normal" traffic and generate an alarm if the actual traffic strongly deviates from the modeled structure.

CBAD was introduced in [11] and its performance in tactical MANETs tested in [12]. CBAD is a graph-based anomaly detection method. All stations participating in the network traffic are represented as nodes in a graph. For all data packets sent in the network, an edge is created between source and destination node of the packet, if it is not already present. For existing edges the weight of the edge is adjusted. To identify the nodes, the IP addresses of the corresponding stations are used. After a specified amount of time (round), this procedure stops, the graph is enhanced using clustering techniques and the structure of the graph is analyzed. Significant differences between the structure of the current graph and preceding graphs indicate an anomaly. The difference of the structure is measured as a so-called *diff* value. Similar to TOGBAD, the estimated mean and the estimated standard deviation are used to derive a threshold for normal *diff* values. *Diff* values exceeding this threshold are considered anomalous. There are two extensions to this basic functionality. The first additionally takes the destination ports of the data packets into account. They are added to the graph as additional nodes. Using this extension, three nodes are created for each packet: one for the source address, one for the destination address and one for the destination port. These nodes are connected via edges. With this extension it is possible to detect activities leading to a high amount of traffic on one port. The second extension is the detection of hyperactivity. If the amount of traffic of one particular node strongly deviates from the normal state, this node is considered hyperactive and thus an alarm is generated.

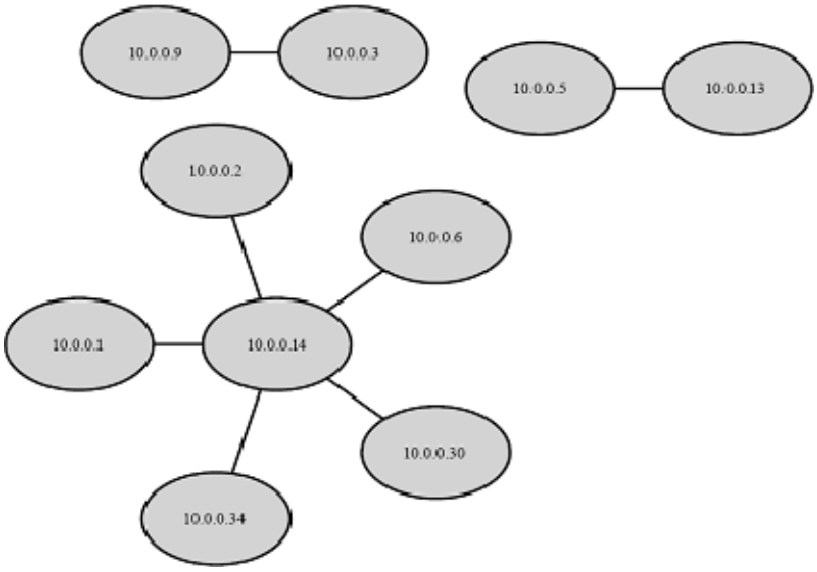

Figure 4: CBAD cluster without attack

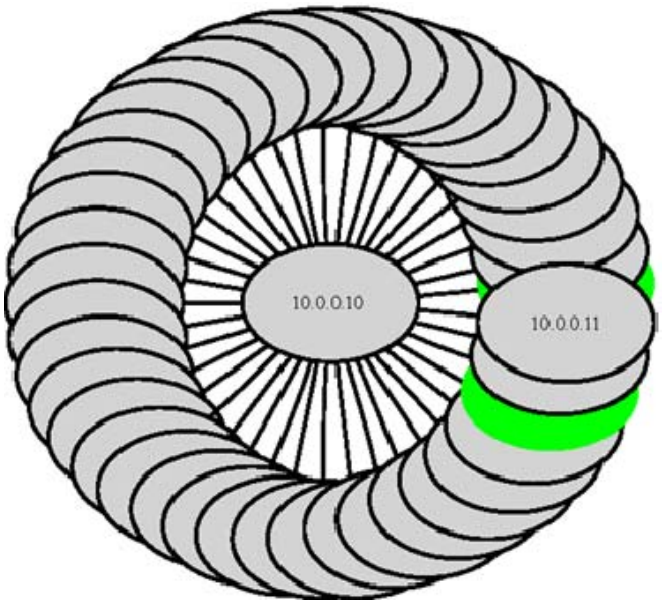

Figure 5: CBAD cluster during worm attack (distribution phase)

Figure 4 and figure 5 each exemplarily show one clustering of CBAD. In figure 4, one clustering without attack and extensions can be seen. Figure 5 demonstrates a clustering during the distribution phase of a worm with the use of the port extension. Ports are represented as green nodes; IP address nodes are gray. Such a clustering is typical for a worm distribution phase, since the worm instances try to spread and thus contact many other nodes. This leads to the formation of big clusters in CBAD as seen in figure 5. The difference between the two figures is obvious and thus the worm attack is detected.

Resource-saving Signature Update Management System (SUMS)

Besides interference or jamming of the wireless communication caused by an opponent, physical takeover of an authenticated MANET node by an enemy or an attack on the MANET routing [13], conventional

attacks known from the field of classical network security also need to be detected in our MANET scenario. Signature-based intrusion detection systems (IDS) are an accepted concept for the detection of attacks on computer networks as known from wired networks. By means of an IDS, special attacks on the network or the nodes can be identified if the characteristic of the attack is known to the IDS in advance. Network-based intrusion detection systems typically conduct network sniffing. Each network packet is recorded and passed through a rule-based analysis stage (cf. [14], [15]). The attack patterns implemented by these rules are called signatures.

Reliability of those IDS is based on continuous updates of the signature database. Usage of outdated signatures would result in making the most current attacks (according to experience, therefore the most prevalent) undetectable. Deploying signature-based IDS in wireless mobile ad hoc networks (MANETs, [16]) adds the demand for efficiency in performing these updates because of the limited bandwidth currently available in wireless networks. Additionally, the special characteristics of ad hoc networks have to be taken into account. The unsteady connectivity for each node and the constantly changing network structure during a mission has to be considered during the design of an update strategy.

The resource-saving Signature Update Management System (SUMS) is a method for efficiently managing the signature updates for the network-based IDS Snort [17] on mobile devices in the MITE scenario. SUMS is based on a client-server architecture which is designed to distribute signature changes in a time-efficient and resource-optimized manner. By using an incremental update procedure, only added, modified, or deleted signatures will be sent to the clients. This is implemented by assigning a serial number, which specifies the order of signature changes chronologically. Based on this, SUMS is able to indicate individually for each client which signatures have changed since the last update. This method minimizes the load on the MANET and the clients.

In MANETs, especially in the MITE scenario, one or more mobile clients might connect to the network only for a short time and signature update packages cannot or can only be transferred partially. Handling such connections using TCP would create avoidable overhead caused by TCP retransmissions as well as renewed connection setup following a connection abort. SUMS use a customized request-response mechanism based on UDP, which is optimized for the special characteristics of ad hoc networks. After a completed update transmission the client can detect which signatures are missing. These signatures can be re-requested separately from the server.

An attacker who distributes wrong or faulty signatures could suspend Snort on all devices in the MANET. For this reason, the SUMS server guarantees adequate security during the transmission of the signatures by digitally signing every package so clients can check the authenticity and integrity of the received signature update.

5 SUPPORTING COMPONENTS AND OPEN IDS SENSOR DETECTOR INFRASTRUCTURE

Because of the semi-autonomous nature of the MANET participants and the unique resource constraints set by the reference scenario, we propose a highly extensible lightweight intrusion detection infrastructure (LII) consisting of sensors and detectors. Inter-component communication is based on the Simple Network Management Protocol with alert messages formatted according to the IDMEF specification. We distinguish between lightweight nodes operated by infantrymen and a more powerful fully-equipped node located in the command vehicle.

SNMP-based Sensor Detector Infrastructure

IDS sensors running transparently on all MANET nodes constantly monitor important properties on the

node itself and/or its environment, e. g. CPU load or GPS coordinates. The sensors' observed data is queried by detectors and analyzed for potentially security-relevant events. Since data should be available to both local and remote detectors, an appropriate communication scheme is required. Due to bandwidth constraints and security considerations, the communication infrastructure needs to be lightweight to reduce network load, and offer authentication and encryption facilities protecting against attackers and eaves-droppers.

The Simple Network Management Protocol version 3 (SNMPv3) is resource-efficient and allows authenticated and encrypted communication. Because it is a well-established protocol for network management, choosing SNMP as the protocol for sensor-detector communication also allows a seamless integration of many already available network management components.

Figure 6 shows schematic diagrams of both lightweight (left) and fully-equipped nodes (right). In the lightweight node, detectors communicate with a local message engine which handles the message exchange with the fully equipped node via SNMP through the MANET. On the fully-equipped node, received messages can be accessed by an IDS console or a threat management system.

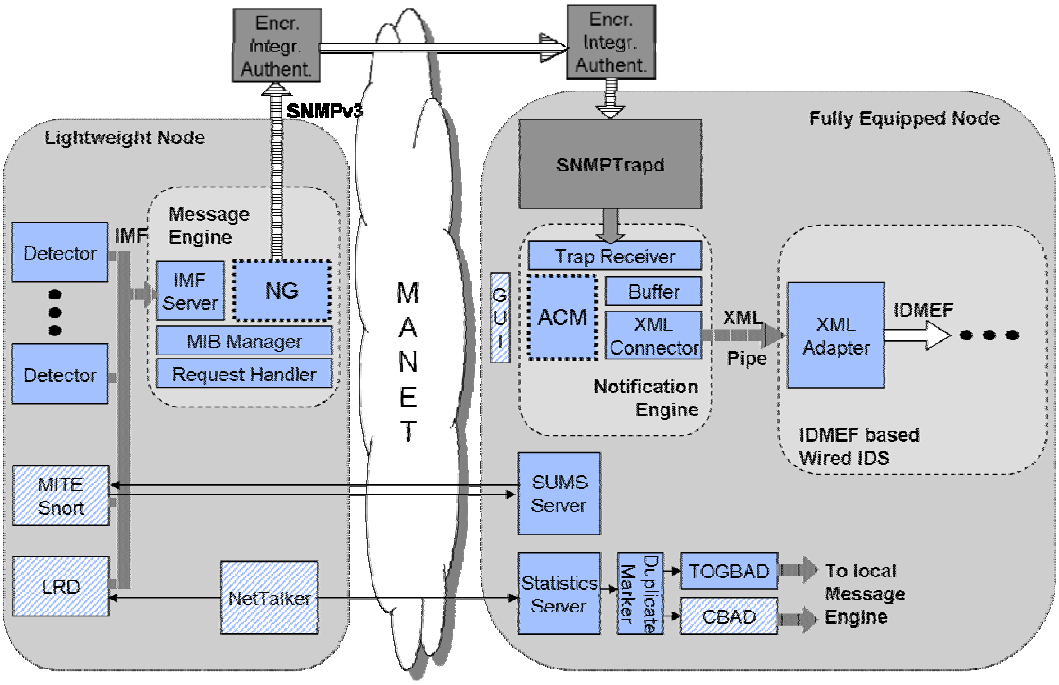

Figure 6: IDS infrastructure with client and server components

Figure 7 shows a more detailed schematic of the SNMP infrastructure on lightweight nodes. On the one hand, all IDS sensors store their observed data in an SNMP MIB. On the other hand, both sensors and detectors read configuration parameters from the MIB and can be configured by changing these values.

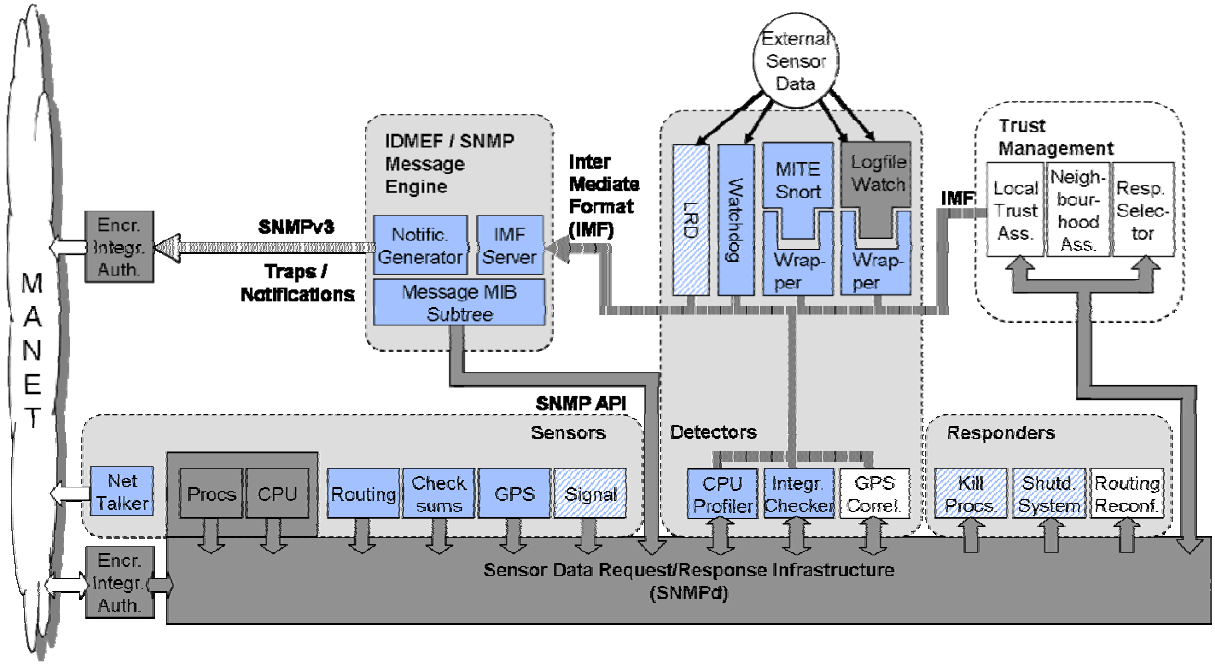

Figure 7: SNMP-based IDS infrastructure on mobile clients

IDMEF-compatible Event Message Handling using SNMP

To be able to send event messages from IDS agents to consoles, it is necessary to have reliable message forwarding, which takes into account MANET-specific network characteristics. The requirements for message forwarding include encryption, authentication, integrity protection, and a low protocol overhead to save network capacity. Event messages should be structured in a widely used, well documented manner to ensure interoperability with third-party components.

For wired IDS, the Intrusion Detection Message Exchange Format (IDMEF, [21]) was standardized by the IETF and guarantees a maximum of interoperability with other IDS components. For MANET use a drawback of IDMEF is the corresponding transport protocol suite (IDXP/BEEP). This protocol suite was primarily designed with respect to the basic conditions of a wired network, thus having relatively high overhead with regard to connection management, while stable long-term connections cannot be guaranteed in a MANET.

SNMP fulfils the general requirements for a transport protocol. Because it uses the connectionless UDP protocol, SNMP generates only a small amount of protocol overhead. Encryption, authentication, and integrity protection can be applied by using the SNMPv3 User-Based Security Model (USM). Reliable transmission can be ensured by using acknowledged SNMP Inform packets for message forwarding.

To ensure interoperability; the proposed IDS uses IDMEF as the basic data structure, while using SNMP as the infrastructure for message forwarding and storage. To make both formats compatible, event messages need to be generated in an IDMEF-equivalent SNMP representation. This is done by the Message Engine on the IDS agent. The Message Engine sends event messages as encrypted, authenticated, and acknowledged SNMPv3 Informs over the MANET to a receiving instance called Notification Engine, where they are converted to IDMEF and made available to the IDS console and/or a GUI that visualizes the current status of the whole network. This communication pathway is illustrated in figure 6.

Using this IDMEF/SNMP communication infrastructure it is possible to reduce the network load even

further by using a tell-and-ask-style communication: On reception of an event message the Message Engine saves the whole message in its local MIB and then only transmits the most relevant event data to the Notification Engine. If more data is required, the Notification Engine may request it by sending multiple SNMP queries back to the agent.

6 EVALUATION RESULTS

This section presents a summary of the evaluation results achieved for the MITE IDS components discussed above. For more in-depth evaluation results, we refer to [12].

Topology Graph-based Anomaly Detection

The evaluation of TOBAD was performed in the network simulator NS-2 [19] as well as in the emulation environment described previously (cf. sect. 2). For simplicity's sake, only the results of the emulative evaluation are presented. The studied scenario is 300 seconds long and consists of 15 MANET nodes in a 300m x 300m area that move at 3.6–10.8 km/h according to the generic motion model. The maximum radio range is set to 150m and both the *random waypoint* as well as the *reference point group mobility* radio propagation models are considered.

After 120 seconds, a randomly selected node starts a black hole attack that is active for 120 seconds. Figure 8 shows the TOGBAD *diff* values for the entire emulation. Green planes indicate that the *diff* value is smaller than the threshold. No alert is generated in this case. Red areas show times during which the *diff* value is higher than the threshold and thus anomalies are detected. For both motion models, the black hole attacks are reliably detected. However, in the case of the RWP motion model, a few false positives are reported. This is due to more strongly fluctuating neighbor relationships. In the case of the RPGM model, anomalies are only detected during the time in which the black hole attack is active.

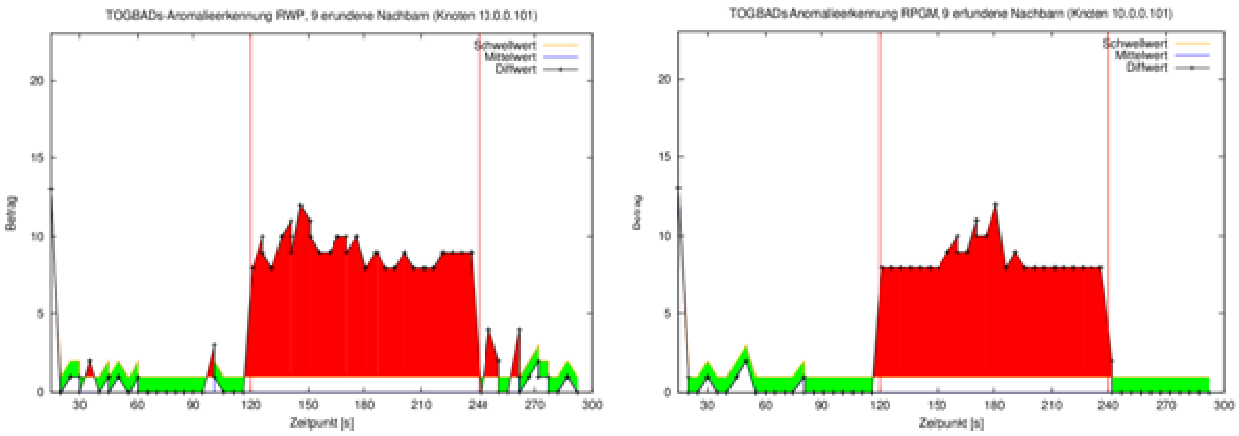

Figure 8: TOGBAD diff values before and during a black hole attack for RWP (left) and RPGM model (right)

Cluster-based Anomaly Detection

Similar to TOGBAD, CBAD was evaluated in a simulative as well as an emulative manner and only the results of the emulation are presented. Since CBAD is capable of detecting a multitude of IP-layer attacks which are often preceded by a port scan, an evaluation of this "preparatory attack" is exemplarily shown.

Figure 9 shows the CBAD *diff* values for both the RWP and the RPGM models during the entire emulation. The port scan starts near round 21 and lasts for three rounds. The port scan is immediately

reflected in the subsequent *diff* value increase. The second peak in the graph indicates the end of the port scan. This is due to the fact that with the currently used parameters, the current clustered graph is compared to that of the last three rounds. Therefore, the end of the port scan also indicates "abnormal" behavior when compared to the behavior during the port scan.

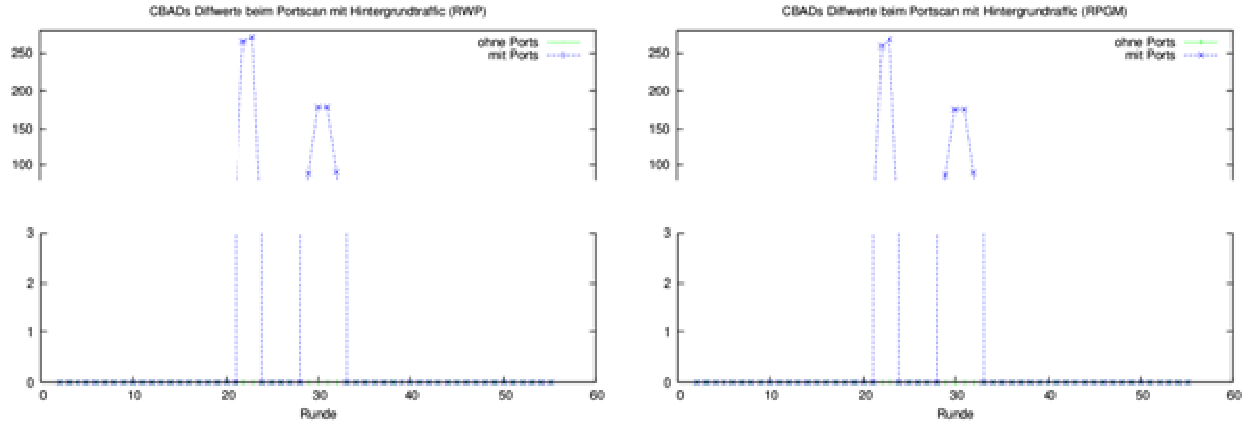

Figure 9: CBAD diff values before and during a port scan for RWP (left) and RPGM model (right)

Local Rule-based Detection

The IDS module for local rule-based detection of routing attacks was evaluated using the network simulator NS-2. The evaluation scenario consisted of 26 nodes in a 1000m x 1000m area with random motion according to the *random waypoint* motion model. The *two ray ground model* was used as the radio propagation model, and the radio range was set to 200 meters. The simulation time was 600 seconds. One dedicated node was used to execute a black hole attack and in a separate simulation run, each other node was used as a detector node.

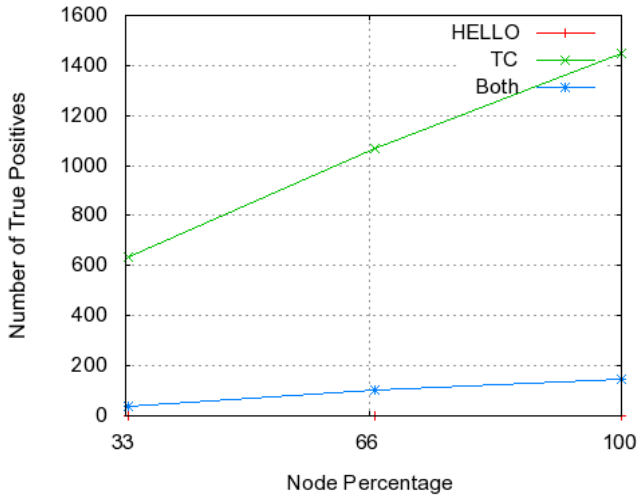

Figure 10: Average aggregated number of generated alert messages for multiple black hole attack variants

Figure 10 shows the average aggregated number of generated alert messages over the falsely propagated number of neighbor nodes (expressed as a percentage of total nodes). An attacker sending only false TC

messages (green line) is detected fairly easily, while the impact of forged HELLO messages is very slight (red line). This is due to the very low probability that the detector node is a direct neighbor of the attacker node. In the case of an attacker sending both fake HELLO and TC messages, there is also an increase in generated alert messages for an increasing number of propagated neighbors, even though the incline is less steep (blue line).

7 CONCLUSION

This contribution has presented the major results of the collaborative MITE research project. The developed solutions (i. e. sensors, detection approaches, and supporting components) have been implemented as parts of a prototypical intrusion detection system (IDS) that is tailored for use in tactical mobile ad hoc networks (MANETs).

The major outcomes of the MITE project include the following: LRD is a locally acting routing message checker that is able to identify violations of the routing protocol's state machine; each of the MANET nodes runs an instance of the LRD. In contrast to this, TOGBAD is a topology graph-based anomaly detection approach that is able to identify routing anomalies by centrally examining received routing messages and observing deviations from a normal profile. Similarly, CBAD is the cluster-based anomaly detector that analyzes the structure of the actually flowing traffic in the network and indicates e. g., abnormal service requests. These centrally acting detectors are fed with information from distributed packet capturing sensors that are also installed on each MANET host. The so-called eWD is an enhanced packet forwarding watchdog that identifies potentially dropped or modified packets which were supposed to be relayed to other nodes.

A resource-saving lightweight intrusion detection infrastructure (LII) has been designed for the necessary information exchange amongst the components of the system. The implementation is mainly based on the Simple Network Management Protocol (SNMP) and realizes robust and low-bandwidth communication processes. Additionally, a highly efficient signature update management system (SUMS) for the open source IDS Snort – that is optionally used as a network-based detector – has been integrated.

Unlike many other research results, the developed components have been demonstrated and evaluated in a real-world implementation environment, based on real hardware and software platforms. This environment honors the impact of node motion and variable node connectivity by using a motion emulator that is based on variable motion sequences and radio wave propagation models. Thus, the MITE project has delivered many successful intrusion detection approaches which have proven their effectiveness and practicability in environments very close to real-world scenarios.

For the near future, different extensions of the system implementation are planned. New detection approaches as well as mechanisms for triggering response actions in a distributed fashion are under development.

REFERENCES

[1] Gerhards-Padilla E., N. Aschenbruck, P. Martini, M. Jahnke, and J. Tölle. Detecting Blackhole Attacks in Tactical MANETs using Topology Graphs. 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. Sep. 2007.

[2] Jahnke, M., J. Tölle, A. Finkenbrink, A. Wenzel, E. Gerhards-Padilla, N. Aschenbruck, and P. Martini. Methodologies and Frameworks for Testing IDS in Ad hoc Networks. In: Proc. of the 2nd ACM International Workshop on QoS and Security for Wireless and Mobile Networks

(Q2SWinet ’07), Chania, Crete, Greece. Sep. 2007.

[3] Jahnke, M., S. Lettgen, J. Tölle, M. Bussmann, and U. Weddige. A Robust SNMP based Infrastructure for Intrusion Detection and Response in Tactical MANETs. In: Proceedings of the GI/IEEE Conference on “Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA2006)”, Berlin, Germany, Jul. 2006.

[4] gentschen Felde, N., J. Tölle, M. Jahnke, and P. Martini. Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System. In: Proceedings of Military Communications Conference (MILCOM 2006), Washington D.C., USA, Sep. 2006.

[5] Jahnke M., C. Thul, and P. Martini. Graph-based Metrics for Intrusion Response Measures in Computer Networks. 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. Sep. 2007.

[6] Jahnke, M., C. Thul, and P. Martini. Comparison and Improvement of Metrics for Selecting Intrusion Response Measures in Computer Networks. In: Proc. of the Sicherheit 2008 Conference, Saarbrücken, Germany, Apr. 2008.

[7] Wang, S., L. Lamont, P. Mason and M. Gorlatova. An effective intrusion detection approach for OLSR MANET protocol. First Workshop on Secure Network Protocols (NPSec), November 2005.

[8] Dhillon, D., J. Zhu, J. Richards und T. Randhawa. Implementation & evaluation of an IDS to safeguard OLSR integrity in MANETs. Proceedings of the 2006 international conference on Wireless communications and mobile computing, 2006.

[9] Ebinger, P. and M. Sommer. Using Localization Information for Attack Detection in Mobile Ad hoc Networks. Sicherheit 2008, Saarbrücken, Germany, Apr. 2008.

[10] Appel, S. and P. Ebinger. Entfernungsschätzungen basierend auf Funksignalstärkemessungen für die Angriffserkennung in MANET. Proceedings of D-A-CH Security 2008. Jun. 2008.

[11] Tölle, J., Intrusion Detection durch strukturbasierte Erkennung von Anomalien im Netzverkehr. PhD thesis, University of Bonn. GCA-Verlag, 2002.

[12] Jahnke, M., A. Wenzel, and G. Klein. Abschlussbericht MITE Phase II. Final report to E/IB1S/6A661/2F005, Jun. 2008.

[13] Jahnke, M. et al. *Research Project Documentation for MITE - MANET Intrusion Detection for Tactical Environments, Project Reference E/IB1S/5A779/2F005*. Federal Office for Information Management and Information Technology of the German Forces (ITAmtBw), 2005-2007.

[14] Haag, J., S. Karsch. *Optimized Sensors for Intrusion Detection in Mobile Ad-Hoc Networks*. Military Communications and Information Systems Conference (MCC), Bonn, Germany, 2007

[15] Wenzel, A. et al. *Verteiltes Packet-Sniffing als Sicherheitswerkzeug in MANETs*. D*A*CH Security, Klagenfurt, Austria, 2007

[16] IETF MANET Working Group. *Mobile Ad-hoc Networks (MANET).* http://www.ianchak.com/manet, April 18, 2008

[17] Sourcefire, Inc. *Snort - Open Source Network Intrusion Prevention System*. http://www.snort.org,

April 18, 2008

[18] Marti, S., T. Giuli, K. Lai and M. Baker. Mitigating Routing Misbehaviour in Ad-hoc Networks. In: Mobile Computing and Networking, pp. 255-265, 2000.

[19] The Network Simulator NS-2. Accessible online under http://www.isi.edu/nsnam/ns/, 2007.

[20] OpenVZ. Accessible online under http://wiki.openvz.org/Main_Page, 2008

[21] Debar, H., D. Curry, B. Feinstein. Intrusion Detection Message Exchange Format - Data Model and Extensible Markup Language (XML) Document Type Definition. IETF Internet Draft draft-ietf-idwg-idmef-xml-14.txt, Jan. 2005.