Response Initiation in Distributed Intrusion Response Systems for Tactical MANETs *

Gabriel Klein, Henning Rogge, Felix Schneider,
Jens Toelle, Marko Jahnke
Fraunhofer Institute for Communication,
Information Processing and Ergonomics FKIE
Wachtberg, Germany
E-mail: firstname.lastname@fkie.fraunhofer.de

Stefan Karsch
Cologne University of Applied Sciences
Gummersbach, Germany
E-mail: stefan.karsch@fh-koeln.de

***Abstract*—Even though Intrusion Detection Systems (IDS) are in wide-spread use, the question of how to efficiently initiate responses to detected attacks has been discussed far less often, especially in highly dynamic scenarios such as tactical MANETs. Despite being flexible and robust in their ability to self-organize, these MANETS are distinctly more susceptible to attacks than their wired counterparts. Especially in military settings such as the interconnection of infantrymen or autonomous robots, remote initiation of countermeasures is critical since local administrative personnel may not be available.**

In this contribution we present an architecture for response initiation that is specifically tailored to the requirements intrinsic to mobile ad hoc networks in these settings. First we introduce IRMEF (Intrusion Response Message Exchange Format) as a means of specifying and parameterizing responses remotely which is an extension of the IDMEF RFC, an experimental yet well-established and recommended IETF draft for formatting event messages. Response initiation messages are dispatched from a central location via a secure, reliable, and robust communication infrastructure based on SNMPv3. An Authenticated Flooding service ensures that messages are delivered to their destination even while the network is under attack. Locally installed responder components are responsible for the application of the response measure.

These mechanisms are designed and implemented explicitly with the limitations in mind which are imposed by the MANET operating environment: For example, resource constraints are taken into account by avoiding bandwidth intensive message formats, and the use of an intelligent flooding mechanism ensures resiliency under routing attacks.

***Keywords*-Intrusion Response, IRMEF, Tactical MANET, Security, IRS Architecture**

I. Introduction

Intrusion Detection Systems (IDS) are in widespread use to monitor various run-time parameters of computer systems and networks in order to detect malicious behavior and other causes of damage and threats.

Appropriate communication protocols are a crucial part of distributed IDSs with respect to reliable transport of event messages, including alerts and heartbeats for indicating that a certain component is up and running. Due to the high demand of interoperability for collecting information from different sources, several standardization activities led to corresponding message format specifications and underlying common data models.

So-called Intrusion Response Systems (IRS, sometimes also referred to as Intrusion Prevention Systems/IPS) extend the IDS capabilities by introducing automatically or semi-automatically triggered measures to respond to detected threats by performing actions such as closing ports or actively terminating network connections.

For distributed IRS, appropriate communication protocols are obviously necessary for initiating response actions at different locations in the network. While using network management protocols such as SNMP is common for reconfiguration tasks, IRS protocol implementations are mostly proprietary (e. g. Cisco IPS Manager for single routers or Cisco MARS which is a network-wide monitoring and threat mitigation system), and there are no known standardization efforts.

Mobile Ad hoc Networks (MANETs) cover a wide variety of non-conventional application scenarios for tactical IP networks, including command post networking, vehicle convoys, autonomous robot sytems, and support for infantry missions. While these networks are very flexible and robust due to their ability to self-organize nodes and routes, they still use an open medium that is susceptible to eavesdropping and other threats.

A limited number of research projects aim at developing IDSs/IRSs for tactical MANETs. They especially address the special requirements of mobile small-scale devices and radio networks in terms of resource efficiency and robustness. Obviously, remote initiation of response actions is absolutely necessary in tactical MANETs, since local administrative personnel is not accessible during missions. The communication protocols need to be extremely reliable, even in situations where the network is partitioned or when attacks against the MANET routing protocols are launched by insiders.

In the cooperative research project *Responsive Intrustion Detection in Tactical MANETs* (RITA, [1]) innovative approaches for detecting insider attacks in tactical MANETs were developed. One of our current research interests is the construction and evaluation of novel countermeasures

* Published in: Proc. of the European Conference on Computer Network Defense (EC2ND). Berlin, Germany, Oct. 2010.

as well as their remote initiation.

After summarizing and discussing existing work in the above context, this contribution presents general and MANET-specific requirements for implementing communication protocols for initiating intrusion response actions, first in a general context and subsequently in tactical MANET environments. After that, a concrete distributed IDS/IRS architecture is described, based on existing standardized or well-established communication protocols. With a few modifications, general IDS message formats are adapted to be used for initiating and parameterizing response actions for detected attacks. We finish with a discussion of these modifications and the additional requirements and consequences.

II. Related Work

Intrusion response is very closely related to network management which deals with "activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems" [2] and can be considered a subset of these measures. Policy-based network management (PBNM) is a specialized approach toward network management that uses operating rules (or policies) to deal with specific situations. PBNM is often found in discussions linked to network quality-of-service (QoS).

RFC 2748 [3] standardizes COPS, the *Common Open Policy Service Protocol*, which uses a client/server-based model for policy enforcement. Clients (policy enforcement points, PEPs) query a central server (policy decision point, PDP) for policy decisions and depending on the returned answer, actions are taken locally. Message transport is realized by piggybacking onto QoS signalling protocols.

Song et al. describe a scalable PBNM framework for MANET management [4] which uses an extended COPS protocol. Nodes are grouped by k-hop clustering and for each cluster there is a single PDP. If two PDPs remain close to each other (with respect to hop count) for longer than a specified length of time, the two clusters are merged and one PDP is eliminated. To preserve bandwidth, PEPs actively and autonomously discover PDPs to associate with.

Similarly, in [5], Hadjiantonis et al. also propose a policy-based framework for MANET management. However, their approach is a context-aware hybrid of a hierarchical and distributed organizational model. They differentiate between lightweight terminal nodes (TN) and more capable cluster managers (CM), where CMs are "collaboratively responsible for the MANET management". A hierarchical element is introduced through the formation of hyper clusters which is a collection of clusters managed by a superior manager node. Distribution is realized by replicating the policy databases on multiple manager nodes, thus introducing a certain resilience.

A method for managing network node configurations by using SNMP is presented by Boros [6]. Traditionally, SNMP-based management was done on a device-by-device basis. However, an SNMP agent can be augmented with a policy management MIB module and a domain-specific policy MIB module (e. g. IPsec) to enable support for PBNM. Thus, a central management instance can issue policies (via SNMP) and local policy MIB modules are responsible for configuring the domain MIB modules (e. g. altering security associations in the IPsec MIB).

Previous work [7] has investigated how an SNMP-based IDS infrastructure would affect the overall communication in MANETs. Most of the analysis results were achieved using software network simulation, and the response portion of the system was only very briefly touched upon. In addition, the experimental implementation of the infrastructure as discussed in [7] neither included possibilities for triggering responses, nor used flooding mechanisms to address multiple nodes and to override the existing routing mechanisms in the presence of routing attacks. However, the proposed datastructures and the transparent translation of messages from XML to SNMP and vice versa is still a fundamental concept of our work.

III. Intrusion Detection Message Exchange

In this section, we introduce well-known message exchange format specifications and related protocols used in the context of intrusion detection systems, both on a technical and procedural level. A more detailed discussion can be found in Section VII.

A. IDMEF

The Intrusion Detection Message Exchange Format (IDMEF, RFC 4765 [8]) defines a data format for sharing information between IDS components. IDMEF describes two message classes that are both represented in XML. While the Alert class is used to send information about detected events, the Heartbeat class is used to regularly indicate the current status of an analyzer.

An alert message consists of information about the analyzer, the message's creation time, and a classification of the alert. Furthermore, it can be extended with several predefined elements such as detection time, analyzer time, source, target, and assessment, and free-form key-value pairs called *additional data*.

A heartbeat message requires only information about the analyzer and the message's creation time, and can be extended with the heartbeat interval, analyzer time, and additional data such as GPS information.

IDMEF—as it is described in its RFC document—does not contain a definition for response messages.

B. IODEF

The Incident Object Description Exchange Format (IODEF, RFC 5070 [9]) defines a data format for exchanging operational and statistical incident information among

Computer Security Incident Response Teams (CSIRTs). One of the design principles of IODEF was compatibility with IDMEF. Thus, IODEF messages are of similar structure and are also represented in XML; however, in contrast to IDMEF, IODEF possesses only one message class. The INCIDENT class is used for all messages and is extremely flexible due to the ability to add or remove optional parameters.

An incident message requires an ID (e. g. an incident tracking number), the report time, a minimum of one assessment and the details of at least one human point of contact. Furthermore, it can be extended with a large amount of predefined elements such as an alternative ID, a related activity, detection time, start time of the incident, a description, the method of how the intrusion was done, event data that gives a description of the comprised events, a history of the incident, and a variable number of free-form key-value pairs called *additional data*.

Because of the large amount of optional parameters IODEF could potentially be reused for response messages. However, IODEF does not provide a small-format message class for periodic messages such as the IDMEF HEARTBEAT class.

C. IDXP

The Intrusion Detection Exchange Protocol (IDXP, RFC 4767 [10]) is an application-level protocol for exchanging IDMEF messages, unstructured text, and binary data between IDS components. IDXP is specified as a Blocks Extensible Exchange Protocol (BEEP, RFC 3080 [11]) which is a generic application protocol for TCP unicast connections. IDXP peers communicate via BEEP sessions, that is, every node has to establish one connection to every other node in the network. Authenticated multicast and flooding are not supported by either IDXP or BEEP.

D. SNMP

The Simple Network Management Protocol (SNMP, RFC 1157 [12]) is a protocol for remotely administrating, configuring, and monitoring network devices from a central location. The IETF standard defines both a data model and an application-layer communication protocol.

Each device maintains its data (in the form of key-value pairs) in a highly extensible so-called *Management Information Base* (MIB) whose elements are arranged in a tree-like fashion. These items are addressed by so-called *object identifiers* (OIDs).

Regular communication between a managed device (agent) and a monitoring instance takes place in a master–slave fashion in which the monitoring instance initiates all communication. Entries in an agent's MIB can be queried and manipulated by using SNMP GET and SET messages, respectively. In case the monitoring instance needs to be alerted, the agent sends either a TRAP or an INFORM message (added in SNMPv2) to the monitoring station. The only difference between the two message types is that TRAP messages are not acknowledged by the receiver.

SNMPv1 and SNMPv2c contained only a rudimentary security mechanism which required the presence of a plain-text "community string" as authentication. Therefore, we utilize SNMPv3 [13] which introduced encryption, authentication, and guarantees message integrity.

IV. Requirements for Protocols to Initiate Intrusion Responses

There are several general requirements for response initiation protocols. Additionally, the MANET context necessitates certain other requirements which are not present in traditional wired environments.

A. General Requirements

The most basic requirement of a response initiation protocol is an adequate addressing scheme that enables targetting of one or more specific nodes that need to apply a countermeasure. Since message recipients can be either single, multiple, or all network nodes, unicast (1 : 1), multicast (1 : n), and broadcast (1 : all) transmission is needed, respectively.

Moreover, the transmission format for response messages needs to be sufficiently flexible to exactly parameterize response measures. An unlimited number of free-form text fields should be available for entering parameters in the form of key-value pairs.

To prevent misuse of the response initiation protocol, certain security mechanisms need to be implemented. To ensure that only authorized network nodes issue response messages, response instructions need to be signed so that their recipients are able to verify the message source's identification. This also serves to ensure that response messages were not modified en route to the recipient. Further, the reinsertion of previously recorded response messages (replay) needs to be suppressed.

Compatibility with existing management and monitoring solutions is another issue that needs to be taken into consideration. Therefore, the use of proprietary formats and protocols should be kept to a minimum.

B. MANET-specific Requirements

Beside the requirements stated in the previous section, the MANET environment has additional drawbacks that a secure and robust response initiation architecture needs to deal with.

Due to the bandwidth restrictions imposed by the shared wireless medium, the communication infrastructure of the intrusion detection/response infrastructure needs to be unobtrusive compared to the other applications operated in the network. Therefore, the format for exchanging intrusion response messages should be as compact as possible.

The open medium further has the drawback that communication can be more easily disturbed than in wired settings.

Therefore, assurances regarding the reliability of intrusion response message delivery have to be given; for example, messages should be able to reach their destination even if the routing situation is disrupted.

Also, for reasons of limited processing capacity on the network nodes (typically PDA-like mobile devices), locally active responder components need to be resource efficient to ensure that other applications running in parallel are not affected.

C. Possible Response Actions

To respond to detected attacks against tactical MANETs, there are different possibilities. Traditionally, all actions which are implementable using remote maintenance or administration tools may be used for responding to attacks, including reconfiguration of the network, the operating system and its subsystems, local or network services, and applications. Table I lists some examples for valuable response actions and their necessary initiation parameters. Note that we focus solely on insider attacks against which we have more leverage than against attacks originating from external sources.

V. Implementation of an Intrusion Response Protocol for Tactical MANETs

In this section, we present our implementation of an intrusion response initiation protocal along with a secure, robust, and reliable communication infrastructure.

A. Intrusion Response Message Exchange Format

As mentioned briefly in Section III-A, the IDMEF definition does not include message classes for specifying responses. For this reason, we introduce the Intrusion Response Message Exchange Format (IRMEF). IRMEF is an extension to IDMEF which adds a RESPONSE class to the message classes of IDMEF.

The RESPONSE class consists of the six elements denoted in Table II. To keep deviation from the IDMEF specification to a minimum, the RESPONSE class uses only elements that are already part of the other IDMEF message classes (see Figure 1).

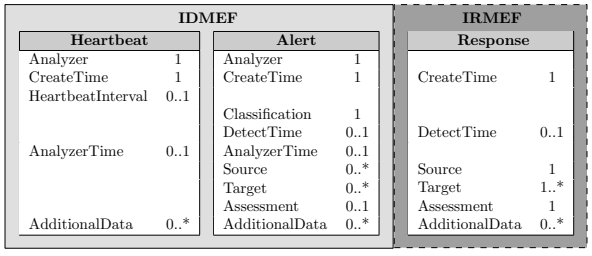

Figure 1. IRMEF extension to IDMEF.

The *CreateTime* field is set to the time the response message is created at the central instance. It serves two purposes: To avoid "old" reponses causing confusion in the network, messages with a timestamp older than a given value are discarded. Also, replay attacks are prevented this way. This is supported by message serial numbers through which repetition of old messages and non-delivery of messages can be detected.

In some cases, the immediate application of a response

Table I
EXAMPLE RESPONSE ACTIONS FOR TACTICAL MANETS.

RESPONSE	DESCRIPTION	PARAMETERS
Lock device display	Lock device display and force the user to reauthenticate	IP address of the attacker node
Revoke different keys	Revoke keys of the attacker node and initiate key renegotiation on the other nodes in order to exclude from encrypted traffic (services, applications, or VPN)	Key-specific ID of the attacker node or its current user
Block ports	Inform all nodes to drop messages from the attacker node on a specified TCP/UDP port	IP address of the attacker node and port number
Exclude from routing	Inform all nodes to drop routing messages from the attacker node	IP address of the attacker node
Adjust routing	Inform all nodes to adjust the routing attractiveness of the attacker node (e. g. by lowering the willingness factor in OLSR) to use the attacker node only for relaying if it is the only connection to other nodes	IP address of the attacker node and adjustment parameters
Kill processes	Shut down malicious processes on the putatively attacked node	Process ID or process table entry of the malicious process
Backup device information	Dump stored information on the attacker device for further investigation	IP address of the attacker node and location of the relevant information
Destroy device information	Delete locally stored information on the attacker device to prevent leakage	IP address of the attacker node and location of the relevant information
Shut down device	Shut down attacker node	IP address of the attacker node

Table II
DESCRIPTION OF HOW IDMEF FIELDS ARE USED IN IRMEF.

FIELD	DESCRIPTION
CreateTime	The time the response was created.
DetectTime	For timed reponses, this is the scheduled time of execution.
Source	The address of the node issuing the response.
Target	One or more addresses of targets that should apply the response.
Assessment	The action that should be performed.
AdditionalData	Contains optional elements that contains parameters for the response to be applied (see Table I).

```
<?XML encoding="UTF-8"?>
<IRMEF-Message>
 <Response messageType="Response" messageid="12">
  <CreateTime>2010-01-17T09:01:27.3</CreateTime>
  <Source>
   <Node>
    <name>console-vn25</name>
    <Address vlan-num="ipv4-addr">
     <address>192.168.0.125</address>
     <netmask>255.255.255.0</netmask>
    </Address>
   </Node>
  </Source>
  <Target>
   <Node>
    <name>agent-vn12</name>
    <Address vlan-num="ipv4-addr">
     <address>192.168.0.112</address>
     <netmask>255.255.255.0</netmask>
    </Address>
   </Node>
  </Target>
  <Assessment>
   <Action>killprocess</Action>
  </Assessment>
  <AdditionalData type="pid">1013</AdditionalData>
 </Response>
</IRMEF-Message>
```

Listing 1. Example response message containing a "kill process" instruction.

might not be required. If so, the *DetectTime* field is set to the time of scheduled execution.

This redefinition of existing fields ensures the compatibility with existing architecture components that are not IRMEF-capable.

A simple example for a response message is shown in Listing 1. In this example, the response consists of the termination of the process with identifier (PID) 1013 on AGENT-VN12. The response is issued by CONSOLE-VN25.

B. Crypto Repository

All applications in the RITA IDS/IRS are equipped with an interface to a storage facility for cryptographic material. With this mechanism we ensure that application-specific cryptographic keys are available when they are needed. Conversely, responses involving key revocation can be similarly implemented by marking them as invalid in the repository.

The described facility is an abstraction from typically implemented key distribution schemes such as *Multicast Internet Key Exchange* (MIKE, [14]). However, the treatment of such mechanisms is outside the scope of our work.

C. IDMEF/SNMP Message Engine

In the RITA distributed IDS/IRS architecture, each node (or agent) has a locally installed message engine that forwards alerts from installed sensors or detectors to a central monitoring instance, or console. At this central location a determination regarding the appropriate response is made (either automatically or manually) and a response initiation message is sent back to the node where a responder component is responsible for the application of the response. Figure 2 highlights these communication paths.

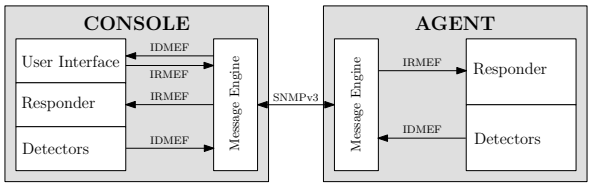

Figure 2. IDS/IRS communication paths in RITA.

Locally, the IDS components communicate with the message engine via IDMEF-compatible XML messages. The canonical method of transmitting IDMEF messages is via IDXP/BEEP (see Section III-C). Because this has severe drawbacks, especially in MANETS, we refrain from using this method. Instead, IDMEF messages are converted into a bandwidth-efficient intermediate format before transmission to the central console. This avoids the communication overhead of transmitting pure XML messages and the necessity of using persistent TCP connections. The messages are then embedded into encrypted and signed SNMPv3 messages. Point-to-point keys for SNMP are extracted from a storage facility for cryptographic material (see Section V-B). We are aware, however, that there might be more efficient manners of message transmission.

On the console side, the message engine is again responsible for recreating IDMEF messages which are passed to a decision-making element. The decision-making process can be either fully automatic, manual, or a mixture of both. In the RITA context, a security console is used to display the current status of the network and manually initiate countermeasures (see Figure 3 for a screenshot).

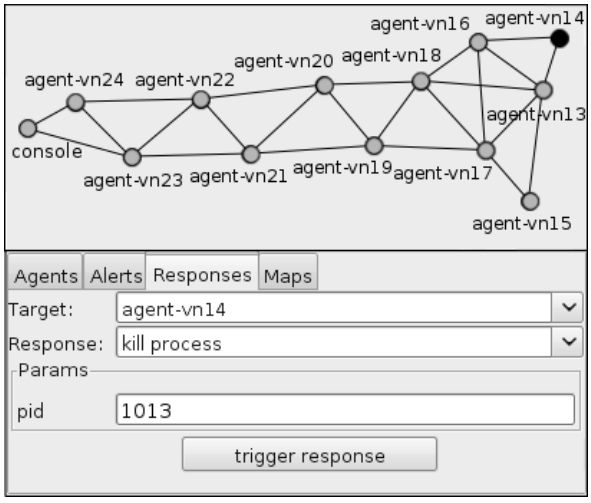

Figure 3. Screenshot of the RITA IDS console application (Helicopter).

In either case, an IRMEF-formatted message (see Sec-

tion V-A) is generated and passed on to the message engine for distribution to the intended recipients. This message contains the type of countermeasure to be applied along with any necessary parameters (e. g. the PID of the process to be terminated). Similar to the reverse direction, the intermediate format embedded in SNMP messages is employed during transmission for bandwidth conservation reasons.

D. Authenticated Flooder

The RITA intrusion response architecture uses a lightweight flooding daemon as a backup routing infrastructure. If an internal attacker manages to disrupt the normal routing daemon, the IDMEF/IRMEF communication switches to flooding for the delivery of messages to their destination. Network routing is assumed to be compromised after a specific number of messages has not been acknowledged, i. e. have not reached their destination. Compared to normal MANET routing protocols, flooding is very robust against misbehaving nodes but consumes more resources for forwarding traffic. Figure 4 shows a comparison between unicast transmission of packets and flooding.

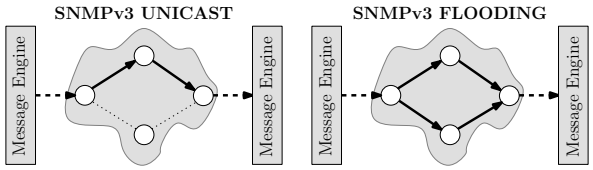

Figure 4. Unicast and flooding in RITA.

Each flooded packet contains an end-to-end authentication header which is checked at every node. The authentication header allows each node to verify the source of the flooded packet and drop the packet if the node has been banned from using the flooding service.

An additional source-specific sequence number is used to detect incoming duplicates and replay attacks. The sequence number is contained in the authenticated part of the packet.

The third security measure is a strict rate limitation for each source. Flooding requires more network resources than normal unicast transmissions in a MANET, so the service could be used by internal attackers to jam the entire network with legitimate traffic. Nodes which send too many packets through the flooder trigger an alert message to the local message engine. Each flooder also checks the rate limitation for its own node to prevent false alert messages on other nodes. The exact rate limit depends on network and mission parameters such as available bandwidth or the necessity of EMCON.

Together, these three security measures protect the flooding channel against unauthorized traffic or internal attackers using impersonation, replay, or denial-of-service attacks by filling the network with legitimate traffic.

Note that the authenticated flooder does not encrypt traffic. It is designed to deliver data to all nodes in the network and if an application such as the message engine uses the flooder as a backup unicast channel it can encrypt the traffic itself to prevent other nodes from eavesdropping on the communication. Additional link-layer encryption for protecting the traffic from outside listeners is beyond the scope of our work.

E. Responder Components

Responder components on each MANET node are responsible for the concrete application of response measures. They register with the local message engine and process incoming messages of type RESPONSE. Upon receipt of a response message, they perform a consistency and a plausibility check to validate the syntax and semantics, and invoke the appropriate local response with the given parameters.

Currently, a single so-called responder daemon is responsible for invoking multiple responses, because this eases the processing load. If there were multiple responder components, each would need to separately process the stream of IRMEF messages and react to those it is responsible for applying. However, multiple responder components are possible and via this mechanism, the system remains easily extensible and new response measures can be easily implemented by plugging a new responder component into the message engine. Thus, basically any type of response can be realized by using system calls, existing libraries, or wrappers for third-party programs.

VI. IMPLEMENTATION AND TESTING ENVIRONMENTS

The target environment for our proposed response initiation protocol is a resource-constrained tactical MANET as used, for example, by infantrymen. A scenario we are examining consists of a hostage rescue mission. In such a scenario, required services are typically command and control information systems (C2IS) and voice/text communications.

To reproduce these circumstances on COTS hardware we have successfully implemented the response initiation protocol on Nokia N810 Internet Tablet devices (400 MHz ARM processor, 128 Mb RAM, 2 Gb flash memory). Due to the lack of an appropriate C2IS implementation, we use a multi-participant navigation system that offers rudimentary C2IS functionality such as display of own forces on a map along with their speed and direction. Communication between nodes is realized by a voice-over-IP service. Neither service is adversely affected by the background operation of intrusion detection and intrusion response mechanisms. To the best of our knowledge, our implementation is the only one which is able to operate transparently in the background.

For testing and evaluation purposes we have also implemented response initiation in our previously described MANET emulation system [15] which allows an arbitrary number of virtual nodes.

VII. Discussion and Conclusion

In our paper we presented an architecture for intrusion response initiation tailored to the specific requirements of tactical MANETS. We suggested the introduction of the IRMEF format which extends the established and often used IDMEF by a RESPONSE class. This extension allows a flexible but exact parameterization of the response measures. It also provides an adequate addressing scheme with respect to the requirements stated in Section IV. However, the choice of SNMP as message transport protocol in our implementation has the drawback that multicast and broadcast messages are currently not possible in practise as SNMP's usage of point-to-point encryption keys does not support multiple message recipients. However, the proposed IRMEF format is very well capable of supporting both message types.

The deployment of a secured SNMPv3 infrastructure for the transmission of bandwidth-efficient ID/IR messages via a resource-saving message engine ensures that security requirements as well as resource requirements are met. For robust and reliable transmission of the response initiation messages a MANET-specific authenticated flooding service was designed and implemented.

The task of policy enforcement in PBNM systems for MANETs may be considered a superset of response initiation in intrusion response systems for MANETs. Existing research on PBNM in MANETs is often focused on the scalable management of large unstructured networks. Therefore, hierarchical approaches for reduced bandwidth and computing resource consumption are suggested.

In typical tactical MANETs we find a small number of nodes combined with a strong demand for secure and reliable transmission of the response initiation messages. This results in gaining almost no benefit by deploying hierarchical approaches for tactical MANETs. Instead, the two-stage model of our approach is even more promising. Under normal conditions the response initiation messages are transmitted via a sparse, specifically designed, message format. Under attack (e. g. when routing is disrupted) the less efficient but very reliable flooding mechanism is used.

The conception and implementation of the intrusion response communication framework has set the ground for further work in the area. We are currently focussing on the automation of intrusion response decisions [16] and a concept for changing of node roles, e. g. a normal node becoming a console node in the case of network partitioning or a previous console node being compromised.

References

[1] M. Jahnke, G. Klein, A. Wenzel, N. Aschenbruck, E. Gerhards-Padilla, P. Ebinger, S. Karsch, and J. Haag, "MITE – MANET Intrusion Detection for Tactical Environments," in *Proc. of the NATO/RTO IST-076 Research Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana, Slovenia, 2008.

[2] A. Clemm, *Network Management Fundamentals*. Cisco Press, Nov. 2006.

[3] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, "The COPS (Common Open Policy Service) Protocol," RFC 2748 (Proposed Standard), Jan. 2000, updated by RFC 4261. [Online]. Available: http://www.ietf.org/rfc/rfc2748.txt

[4] W. Song, S. Rehman, and H. Lutfiyya, "A scalable PBNM framework for MANET management," in *IM'09: Proceedings of the 11th IFIP/IEEE international conference on Symposium on Integrated Network Management*. Piscataway, NJ, USA: IEEE Press, 2009, pp. 234–241.

[5] A. Hadjiantonis, A. Malatras, and G. Pavlou, "A context-aware, policy-based framework for the management of MANETs," in *POLICY '06: Proceedings of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 23–34.

[6] S. Boros, "Policy-based network management with SNMP," in *Proc. of EUNICE*, University of Twente, Twente, Netherlands, 2000.

[7] M. Jahnke, J. Tölle, S. Lettgen, M. Bussmann, and U. Weddige, "A Robust SNMP based Infrastructure for Intrusion Detection and Response in Tactical MANETs," in *Proceedings of the GI SIG SIDAR Workshop on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2006)*, ser. LNCS, R. Büschkes and P. Laskov, Eds., vol. 4064. Berlin, Germany: Springer-Verlag, Heidelberg, Jul. 2006, pp. 164–180.

[8] H. Debar, D. Curry, and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)," RFC 4765 (Experimental), Mar. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4765.txt

[9] R. Danyliw, J. Meijer, and Y. Demchenko, "The Incident Object Description Exchange Format," RFC 5070 (Proposed Standard), Dec. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc5070.txt

[10] B. Feinstein and G. Matthews, "The Intrusion Detection Exchange Protocol (IDXP)," RFC 4767 (Experimental), Mar. 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4767.txt

[11] M. Rose, "The Blocks Extensible Exchange Protocol Core," RFC 3080 (Proposed Standard), Mar. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3080.txt

[12] J. Case, M. Fedor, M. Schoffstall, and J. Davin, "Simple Network Management Protocol (SNMP)," RFC 1157 (Historic), May 1990. [Online]. Available: http://www.ietf.org/rfc/rfc1157.txt

[13] U. Blumenthal and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)," RFC 3414 (Standard), Dec. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3414.txt

[14] T. Aurisch, T. Ginzler, and P. Martini, "Practical efficiency analysis of a dual mode group key management," in *Proceedings of the 2008 Military Communications Conference (MILCOM)*. IEEE, 2008.

[15] H. Rogge, G. Klein, A. Wenzel, and M. Jahnke, "Improvement of IP-based MANET emulation," in *Proceedings of the 2009 Military Communications and Information Systems Conference (MCC)*, Prague, Czech Republic, 2009.

[16] M. Jahnke, "Graph-based automated denial-of-service attack response," PhD Dissertation, Rheinische Friedrich-Wilhelms-Universität Bonn, Bonn, Germany, 2009.