Intrusion detection system and response for mobile ad hoc networks

Dan Nordqvist, Lars Westerdahl,
Anders Hansson

FOI-R--1683--SE
ISSN 1650-1942

Command and Control Systems
User report

July 2005

FOI is an assignment-based authority under the Ministry of Defence. The core activities are research, method and technology development, as well as studies for the use of defence and security. The organization employs around 1350 people of whom around 950 are researchers. This makes FOI the largest research institute in Sweden. FOI provides its customers with leading expertise in a large number of fields such as security-policy studies and analyses in defence and security, assessment of different types of threats, systems for control and management of crises, protection against and management of hazardous substances, IT-security an the potential of new sensors.

FOI
Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping

Tel:
Fax:

www.foi.se

Intrusion detection system and response for mobile ad hoc networks

FOI-R--1683--SE
ISSN 1650-1942

Command and Control Systems
User report

July 2005

Issuing organization FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	**Report number, ISRN** FOI-R--1683--SE	**Report type** User report
	Research area code 41 C4I	
	Month year July 2005	**Project no.** E793055
	Sub area code 41 C4I	
	Sub area code 2	
Author/s (editor/s) Dan Nordqvist Lars Westerdahl Anders Hansson	**Project manager** Elisabeth Hansson	
	Approved by Martin Rantzer	
	Sponsoring agency FMV	
	Scientifically and technically responsible Elisabeth Hansson	
Report title Intrusion detection system and response for mobile ad hoc networks		
Abstract (not more than 200 words) The research area of mobile ad hoc intrusion detection systems (IDS) is still under development. Existing IDS'es are mainly for wired or wireless networks. In a previous report it was concluded that existing products for wireless IDS'es are not suitable for tactical mobile ad hoc networks. The IDS architecture of the tested tools neither has support for the autonomous and self-organized property nor the ability needed for detecting relevant attacks. In this report an architecture for a mobile ad hoc network IDS is presented. The IDS is based on requirements from a general perspective, some special requirements for the ad hoc environment and finally military requirements. The result is a network IDS located on each node within the network.		
Keywords IDS, ad hoc, mobile networks		
Further bibliographic information	**Language** English	
ISSN 1650-1942	**Pages** 34 p.	
	Price acc. to pricelist	

Utgivare FOI - Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--1683--SE	**Klassificering** Användarrapport
	Forskningsområde 4. Ledning, informationsteknik och sensorer	
	Månad, år Juli 2005	**Projektnummer** E793055
	Delområde 41 Ledning med samband och telekom och IT-system	
	Delområde 2	
Författare/redaktör Dan Nordqvist Lars Westerdahl Anders Hansson	**Projektledare** Elisabeth Hansson	
	Godkänd av Martin Rantzer	
	Uppdragsgivare/kundbeteckning FMV	
	Tekniskt och/eller vetenskapligt ansvarig Elisabeth Hansson	
Rapportens titel (i översättning) Intrångsdetektering och svar för mobila ad hoc nätverk		
Sammanfattning (högst 200 ord) Forskningsområdet intrångdetekteringssystem (IDS) för mobila ad hoc nätverk är under utveckling. De existerande IDS:er som finns på marknaden är i huvudsak avsedda för fasta och trådlösa nätverk. I en tidigare rapport framkom det att existerande produkter för trådlösa IDS:er inte är lämpliga för taktiska ad hoc nätverk. Arkitekturen i dessa verktyg stödjer inte behoven av autonoma och självorganiserande nätverk samt saknar förmågan att upptäcka relevanta attacker. I den här rapporten föreslås en arkitektur för en mobil ad hoc IDS. Systemet är baserat på generella IDS krav likväl som på specifika krav som uppkommer med ad hoc miljön. Militära krav är även infogade i arkitekturen. Resultatet är en nätverks IDS implementerad i samtliga noder i nätverket.		
Nyckelord IDS, ad hoc, mobila nätverk		
Övriga bibliografiska uppgifter	**Språk** Engelska	
ISSN 1650-1942	**Antal sidor:** 34 s.	
Distribution enligt missiv	**Pris: Enligt prislista**	

Index

List of Figures

List of tables

1 Introduction

Security in networks is achieved in different manners and in different ways with the use of various techniques. Encryption is one of the oldest and most generally accepted methods of providing security to an information system. However, encryption cannot by itself provide every aspect of the needed security in a network in general, much less in a military mobile ad hoc network.

In its most generic term, security is described using the words confidentiality, integrity and availability. In some cases non-repudiation is added. Encryption is an excellent example of confidentiality since the purpose of encryption is to keep something secret. Keeping something secret is not the only thing that is important though, it is often just as important to know if someone has discovered the secret or is trying to do so. Thus, a system for discovering attempts or ongoing attacks towards the system is also needed.

Initially intrusion detection systems (IDS’es) operated on wired systems. From a network point-of-view that meant that the actual supervision could more or less be implemented. As wireless systems got more popular, IDS'es evolved to handle this new infrastructure. However, technically wireless only means that there are a few given positions on the network to monitor. The communication media changed with wireless but not necessarily the infrastructure.

In a mobile ad hoc-environment the static behaviour is not reliable. The term ad hoc implies temporary solutions or, in this case, topologies. It is in most cases predetermined which applications that will communicate with each other but not where the applications will be physically. The route from sender to receiver may vary between each transmission. Thus, the requirements on mobile ad hoc IDS vary some compared to traditional IDS.

In a previous report, FOI compared available IDS products for wireless networks. All of the tested product where found lacking in their ability to handle an ad hoc situation. This report will provide an architecture for a mobile ad hoc network.

1.1 Motivation

This project is also part of a project agreement between Sweden, the Netherlands, and Canada (Projekt agreement, 2003). Canada describes problems and proposes solutions within the area of authentication for mobile ad hoc networks. The Netherlands investigate whether it is possible to create a boundary protection for mobile ad hoc networks. Sweden contributes within the area of intrusion detection systems (Hansson & Hansson (2004) and this report). As a result of the collaboration we have agreed on the following assumptions:

1. Base security measures are offered by the physical and the data link layers.
2. Discretionary measures (written in italic in Figure 1) are defined by the security policy for the network layer and above.
3. Nodal intrusion detection is used as a second line of defence.
4. In order to limit the user’s interaction with the device some automation is required. The device holds security features e.g. intrusion detection or authentication code for automated responses.

Security protocols discussed within the collaboration is listed in Figure 1.

1.2 Problem description

Previous intrusion detection systems have mainly focused on wired or, at least, static networks. These networks have wires or, in case of wireless, access point which are easy to identify. A traditional network IDS is typically situated and optimized for a wire or an access point. As a result those systems are note quite suitable for a mobile ad hoc-environment where the structure and topology is not possible to predetermine. In this report, requirements and a theoretical model of mobile ad hoc intrusion detection system is presented.

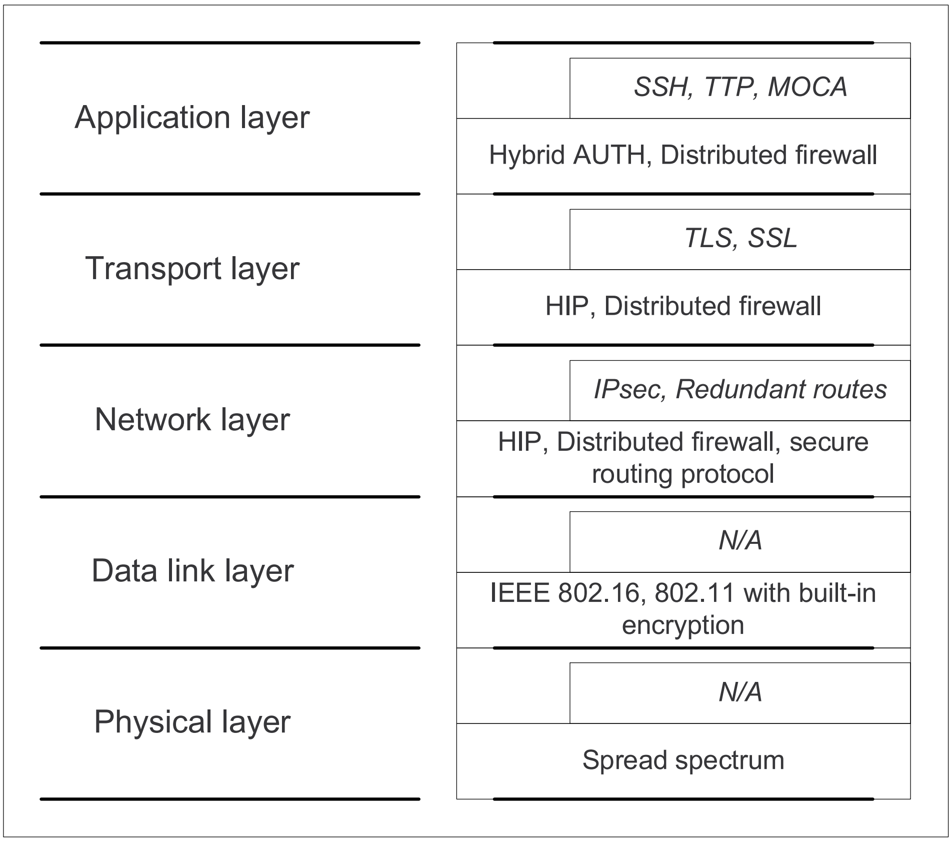
Application layer
SSH, TTP, MOCA
Hybrid AUTH, Distributed firewall
Transport layer
TLS, SSL
HIP, Distributed firewall
Network layer
IPsec, Redundant routes
HIP, Distributed firewall, secure routing protocol
Data link layer
N/A
IEEE 802.16, 802.11 with built-in encryption
Physical layer
N/A
Spread spectrum

Figure 1. A basis for a security concept architecture.

1.3 Limitations

A tactical ad hoc network may take many forms. It is not necessarily an IP based network or even based on an operating system that we used to today. In this report however, we will describe the situation where we use the traditional TCP/IP-stack. The main reason for this is the range of commercial and open source products and standards available.

1.4 Results

The result of Sweden’s contribution to the agreement is a network-oriented IDS that is attached to each node within the mobile ad hoc network. Thus the IDS is present throughout the whole network without creating bottlenecks.

Internally the IDS main tool is a specification-based detector with the use of a misuse detector as a backup.

The IDS can respond to attacks by either excluding neighbouring nodes or, if possible, by contacting a central server for a stronger response such as re-keying or revocation of nodes.

1.5 Report layout

Section 2 gives a general overview of intrusion detection techniques and other technologies that affect the efficiency of the IDS. Section 3 outlines the requirements for an IDS in a tactical ad hoc network. In section 4, an architecture based on the requirements in section 3 is presented. Finally, section 5 provides some insight in future possibilities.

2 Intrusion Detection Systems

An intrusion detection system operates differently depending on the underlying infrastructure of the system. The difficulty and the manner in which it is done vary with the technology being implemented. One of the first and the most obvious difference between a traditional IDS and a mobile ad hoc IDS is the lack of cables in the latter. In a wireless system it is hard to avoid eavesdropping. Although it might not be possible for an eavesdropper to understand what is being said she can record the communication and do traffic analysis later or she can retransmit messages in a replay-attack. In the latter example it is not even necessary to understand what is being transmitted.

A wireless network has, to a certain extent, a fixed backbone system. That is, the wireless components communicate with an access point, which has a central position in the wireless infrastructure. Thus, the access point provides a given node where the network communication passes. Ideally, a network IDS should monitor such a node.

Mobile Ad hoc networks are usually wireless as well but has not always access to a fixed backbone system like the wireless system described above. Thus there is no obvious node to where to monitor the network.

In this section the large prerequisites for an IDS is described and will lay as a foundation when the architecture is presented later.

2.1 Infrastructure

Network infrastructures can be viewed as either centralized (sometimes called hierarchical) or decentralized. A centralized structure is typically a client-server system where the server provides all the functionality and the clients ask the server for everything they need or report to the server if they have discovered something interesting. The good part with a centralized infrastructure is that it is easy to supervise. The server is the brain of the system, thus updates are distributed from one location. That also means that the bulk of all communication will pass through the same location. From the clients point-of-view the server is the only place a client has to turn in order to get updates, verification of certificates et cetera.

The downside of a centralized structure is based on the same properties as the upper side. Having a point with all the power and knowledge in the system results in a single-point-of-failure. That is, the server represents an obvious target which, if an attack is successful, will cause severe harm to the entire network.

In a fully distributed network there is no single-point-of-failure present. Having the functionality spread out over the network provide survivability if a part of the network is attacked. If one or a few nodes are compromised, it will not affect the rest of the network in a catastrophic way. However, the distributed nature makes the network difficult to supervise. It becomes increasingly harder to maintain a defined and guarantied level of protection throughout the network.

Table 1. Summary centralized and distributed infrastructure.

	Centralized	Distributed
Pros.	• Easier to monitor • Easier to maintain	• High survivability
Cons.	• Single point of failure • Obvious target	• Difficult to supervise • Difficult to maintain

When studying the requirements, it is clear that the IDS solution should be distributed. However, a purely distributed solution is difficult to secure. A high level of distribution also means that the individual nodes in the network should collaborate to a certain extent. The existing methods and protocols for this are to date not trustworthy enough from a security point-of-view. Thus, a hybrid solution that takes advantage of the good properties of both centralized and decentralized infrastructures is preferable.

Ad hoc by its nature means distributed. The lack of centralized nodes and the requirement for not enforcing such nodes results in a solution where an IDS is situated on each node.

2.2 Type of detectors

To provide monitoring of a network and detection of both known as well as unknown attacks, an IDS needs to operate close to real-time. That means that the IDS must run automatically and that human supervision is kept at a minimum.

2.2.1 Misuse/signature-based detection

The first IDS'es where typically log analyzers used to determine what had already happened. A common method for this was to look for patterns (Kumar, 1995) of events in a log. This is typically called misuse or signature-based detection. The method is effective in the sense that the detection rate is high and that there usually is a low rate of false alarms. Also, with the hardware available today the log analysis can be performed at a speed close to real-time.

A major drawback with misuse/signature-based detection is that the IDS have to know what a given attack looks like. Thus it is not a good method for discovering unknown attacks.

Table 2. Misuse/signature-based detector.

Pros.	Cons.
• Usually high detection rate and low false alarm rate (if updated) • Performs in real-time • Does not demand a lot of resources • Open source, freely available	• Must be updated with new signatures regularly • Does not handle unknown or previously unrecorded attacks • Many rules • Does not know of routing attacks and military apps

2.2.2 Statistical-based anomaly detection

In resent years anomaly detection has become a popular topic in IDS research. The idea with anomaly detection (Kumar & Spafford, 1994) is that the IDS shall identify abnormal behaviour by the user or the overall system. The IDS compares a defined normal state with the actual state of the system.

The idea with anomaly detection is appealing but the method has many drawbacks. It is expensive when it comes to system resources, and it is not very reliable. On the upper side, it has the potential to detect unknown attacks.

Table 3. Anomaly/statistical-based detector.

Pros.	Cons.
• Easy to implement (all magic done by the algorithm) • Detects unknown attacks	• High false alarm rate • Resource intensive • Often too slow to run in real-time • Needs to train detector on prepared data (overtraining possible) • May be sensitive to radio silence (not normal behavior) • Must be retrained when introducing new tools or updated versions

2.2.3 Specification-based anomaly detection

Specification-based detection (Ko et al., 1994) crosses the line between signature-based detection and statistical anomaly detection. But where signature-based detection do pattern-matching with known attacks and anomaly detection looks for deviations, specification-based do pattern-matching on a description of how an application is supposed to behave.

Using a signature of a reliable state is much more efficient and inexpensive when it comes to resources utilization. In many aspects, specification-based detection is a form of anomaly detection.

Table 4. Specification-based detector.

Pros.	Cons.
• Small and fast implementation, performs in real-time • Not so resource intensive • Possible to get 100% detection rate and no false alarms, even on unknown attacks (if the rules are correct) (Uppuluri & Sekar, 2001). • Successful tests has been performed at FOI with an implementation of AODV routing attacks detection • Can also handle known attacks if they can be described by the rules	• Hard to implement good rules from specifications, but there should be implementations available that can be reused. • Might react different in reality compared with the specification, since an implementations interprets specs. But this is relatively easy to patch! • Needs new rules when adding new tools, and possibly for updated versions.

2.3 Cryptology

This chapter describes how cryptography affects the IDS. The focus here is not to find the ideal cryptographic solution, but rather to explore how different methods of cryptography affect the operation and the efficiency of the IDS.

Cryptography can be described in manners. One way of describing it is to look at what part of the message is encrypted and where. This is commonly known as node-to-node and end-to-end encryption.

In node-to-node encryption the message is encrypted when moving between nodes, i.e. when it is "in the open". At each intermediate node the message is decrypted, read (the header anyway) and encrypted again before passing the message along.

End-to-end encryption provides an encrypted block which remains encrypted throughout the whole route from sender to receiver. The content is kept secret from any intermediate node. Figure 3 depicts the difference between node-to-node and end-to-end cryptography.

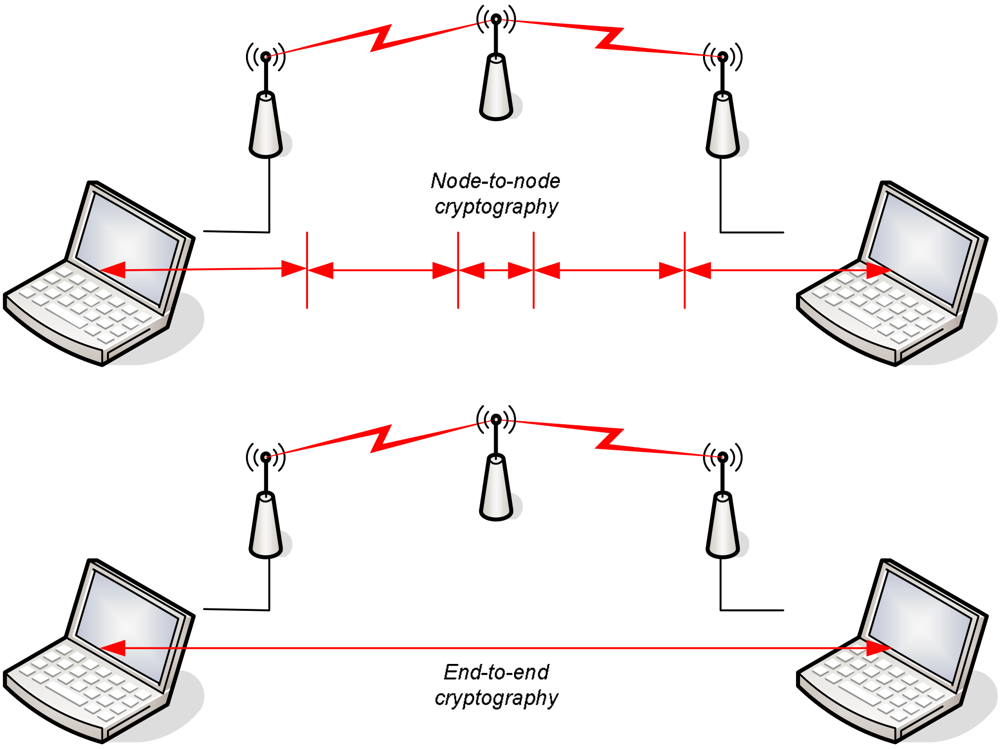

Figure 2. Encryption modes.

The description of node-to-node and end-to-end encryption encloses the layers in the TCP/IP-stack. A node-to-node encryption is typically accomplished by the link layer. End-to-end encryption on the other hand can be accomplished in various manner by the other layers in the stack; network, transport or application.

2.3.1 Link layer cryptography (node-to-node)

Link layer encryption provides node-to-node encryption. This means that the data is encrypted when travelling from one node to another. When the encrypted message reaches an intermediate node the message is decrypted so the intermediate node can determine whether to keep or to forward the message. Before forwarding the message it is re-encrypted again. A consequence of link layer encryption is that the message is vulnerable for compromised nodes.

A typical use of link layer encryption can be within a group. If all members of a group share an identical symmetrical key they can use this key for link layer encryption. The benefit of using node-to-node encryption with a symmetric group key is speed. A drawback is that there is no individual identification.

Usually, these operations are conducted without the involvement of higher layers within the TCP/IP-stack. It is however imperative for the mobile ad hoc network that the communication information utilized at this layer is made available for the IDS in order for the IDS to be able to detect low level deviations.

2.3.2 Network layer cryptography (end-to-end)

End-to-end cryptography means different things for the layers above the link layer. From the network layers point-of-view the “end” is the node of some sort on the receiving side. The node can be the destination network or a host on that network. It is not necessarily the same as a certain application or user.

An example of network layer encryption is IPsec. IPsec can be used for both encryption as well as authentication. The Encapsulating Security Payload (ESP) service in IPsec operates in transport mode or in tunnel mode. The transport mode encrypts the payload of the packet while maintaining the header unchanged. In tunnel mode IPsec encrypts both header and body of the packet and generate a header of its own. In doing so IPsec hides the actual receiver (host) of the packet while presenting the destination network to intermediate nodes.

The IDS must be able to catch packets in different modes in order to examine IPsec packets.

2.3.3 Transport layer cryptography (end-to-end)

Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) are the dominant protocols for providing security at the transport layer. Both uses mutual authentication with public keys and symmetric keys for constructing a tunnel between sender and receiver. After an SSL/TLS connection has been set up the protocols provide a secure transport for packets from sender to receiver.

The primary use of SSL/TLS has been for web browsers. For an IDS to handle SSL/TLS packets it has to be invoked at the end of the SSL/TLS tunnel, thus catching the packets between the tunnel and the requesting application.

2.3.4 Application cryptography (end-to-end)

An application can encrypt a message. Application-to-application encryption is the purest form of end-to-end encryption since the payload of a message only will be visible in plaintext to the receiving application. Thus it is only the sender and, arguably, the receiver of the message that will be able to understand the content.

One major difference between applications in the application layer and other applications in lower layers is that there is not necessarily a defined format of how an application shall operate. It may be difficult for an IDS to catch application layer encrypted traffic if the protocol does not provide openings for the IDS to examine the content.

2.4 Responses to detected Intrusions

Detected intrusions in a network should generate alarms to users or administrators and also generate system log records for later analysis. This is useful together with security policies describing the human actions to be taken in response to attacks (Kossakowski, 1999).

During critical phases of tactical operations, on the other hand, there may be a great need for very short-term automatic actions that can block, or at least reduce the damage of an ongoing communication attack. Automated responses for wired networks are discussed in (Hawrylkiw), (Larsen & Haile, 2002) and (Carlinet, 2004) with examples on how the communication from the malicious node can be disrupted by TCP RESET packets, ICMP error messages or firewall rule manipulation. Unfortunately, these responses can be by-passed or used to disrupt communication to innocent nodes.

While a network with automated intrusion response will have much greater likelihood of interrupting an intrusion in progress, it will, on the other hand, run the risk of falsely reacting against valid usage due to false alarms. It is important to avoid countermeasures in the case where a node or user is doing something unusual or suspicious, but for honest reasons.

Two other problems must be considered in the design of automated intrusion responses. The first is how to avoid misdirected responses to legitimate users by identity spoofing or false detections. The second problem is how to safeguard responses that require much network, power or user resources from being exposed to denial-of-service attacks.

2.4.1 Proposed response principles

We suggest that nodes perform responses without collaboration with other nodes, since it is still an open problem whether collaborative responses can be implemented without weakening the security in the ad hoc network. Responses can be local, only involving the detecting node itself, while global responses are directed to all nodes in the ad hoc network. Global responses are only allowed to be initiated from a centralized IDS server in the network. In some situations, the IDS server cannot be used, for example due to bad transmission conditions, low network capacity or radio silence mode. Then only local responses can be performed. The choice of response depends on the type of attack.

Responses can be classified as weak or strong, depending on their efficiency and their impact on the network, power or user resources. When an intrusion is detected, the node can either initiate weak local responses or inform a centralized IDS server about the attack if it is accessible. In addition, local user re-authentication requests (a strong local response) can be performed when necessary.

2.4.2 Example of weak local responses

Local responses are fast since no communication between nodes is needed. Preferably, they are performed at a lower layer or at least within the same layer as the attack. Responses can be performed within the attacked protocol, for example by dropping malicious route packets and updating the node’s routing table in order to avoid routing to or from the adversary. Other examples of weak local responses are to drop packets before they are processed by the MAC layer (in case of collision attacks or other MAC-layer attacks) or to warn the end user of the intrusion. If the node is not needed for a while, the user can then decide to restart the node in a safe mode for maintenance and system analysis. Whether on-line maintenance can be performed at the same time as the node is used must be studied further.

2.4.3 Examples of strong global responses

From (Zhang & Lee, 2000) and (Mishra et al., 2004), we have three examples of strong responses:

1. As a result of a forced re-keying at the wireless interface on the data link layer, the wireless network will be reinitialized and the malicious node will not have wireless access any more.
2. Identify the compromised nodes and force a reorganization of the routing paths in the network in order to avoid malicious traffic.
3. All users in the network are requested to re-authenticate themselves.

2.4.4 Conclusion

Efficient and secure active responses are much more important in tactical mobile ad hoc networks than in commercial networks. There are no studies on the consequences of using active responses in mobile ad hoc networks in the literature. Although we give some examples on different types of response, there is need for further research in this area.

2.5 Problems with current wireless IDS tools

In Hansson & Hansson (2004) a survey was made over currently available IDS tools. It was concluded that they, in general, were best suited for corporate wireless networks where there are some fixed nodes in the infrastructure. Also, the response time is slow due to the fact that the logs have to be examined by the network administrator.

The ability to discover unknown attacks was limited. This became apparent when it was concluded that the tools was not able to detect dedicated attacks towards mobile ad hoc protocols.

3 Requirements

The requirements for an mobile ad hoc IDS was described in Hansson & Hansson (2004) and are summarized here. The requirements are divided into:

- General requirements, which are requirements applicable for IDS in general
- Specific requirements, which are requirements applicable for ad hoc networks
- Military requirements, which are requirements based on the operational environment

3.1.1 General requirements

An IDS working under ideal circumstances is transparent to the user of the system. For the IDS to be transparent it has to be reliable. Being reliable means that, apart from detecting attacks, it should not generate false alarms every now and then. Reliability is a key issue when it comes to the operators' trust of IDS. Trust for the system is hard to formulate as a requirement but it is a very important property when it comes to describing or evaluating the efficiency of the system.

Hansson & Hansson (2004) denotes the general requirements for the IDS proposed in this report.

Table 5. General requirements.

Req.no.	Name	Description
GR01	Automatic detection	The IDS shall automatically detect known attacks and be able to detect unknown attacks
GR02	Powerful automatic response	The IDS shall provide automatic response to attacks without human intervention
GR03	Fault-tolerant and attack resistant	The IDS algorithms shall be robust and fault tolerant to resist attacks on the IDS itself
GR04	Only system administrator may configure and modify settings	Only authorized personnel shall be able to configure the IDS
GR05	Transparency	The IDS shall run continuously and by transparent to both the system and the user
GR06	Low false rate, high detection rate	To maintain credibility the system must be accurate and reliable
GR07	Not introduce new weaknesses	The IDS shall not expose the node in any new way
GR08	Scalable	The IDS shall be scalable

3.1.2 Specific requirements

A mobile ad hoc solution has some special needs to take into account. Hansson & Hansson (2004) identify the following requirements.

Table 6. Specific requirements.

Req.no.	Name	Description
SR01	Autonomous and self-organizing	The IDS shall be able to operate in a self-organized network and in an environment where no fixed infrastructure exists
SR02	Economy	The technology shall use resources efficiently and provide low overhead
SR03	Detect attacks on all layers	The IDS shall be able to operate on any level in the TCP/IP stack including attacks that are typical of mobile ad hoc networks.
SR04	Identify malicious nodes	The IDS shall be able to detect malicious behaviour by neighbouring nodes

3.1.3 Military requirements

The nature of military operations today involves a high degree of collaborations and temporary units that only exists during a specific operation. Thus mobile ad hoc networks are ideal for military purposes. The flexibility of a mobile ad hoc network provides a good base for establishing communication between units that normally do not communicate. However, the flexibility is also the weakest point in the system, since it is hard to predict which nodes that will communicate within the network.

In Hansson & Hansson (2004) a set of military requirements on an ad hoc intrusion detection system is specified. A summary of these requirements is given below.

Table 7. Military requirements.

Req.no.	Name	Description
MR01	Automatic response	The response time should not be more than a few minutes
MR02	Attack detection	The type of attacks may differ from common situations. The IDS shall be able to detect new attacks including halting as well as degrading attacks.
MR03	Distributed protocols	The IDS should not be dependent on a central server
MR04	Survivability	The IDS should be able to perform under poor network conditions
MR05	Radio silence	The IDS shall not be able to communicate outwards when radio silence is preserved.

3.1.4 Summary requirements

Some of the requirements identified above are redundant and they all represent requirements on different technical levels. As a summary of the requirements a generalised form of the requirement is presented here.

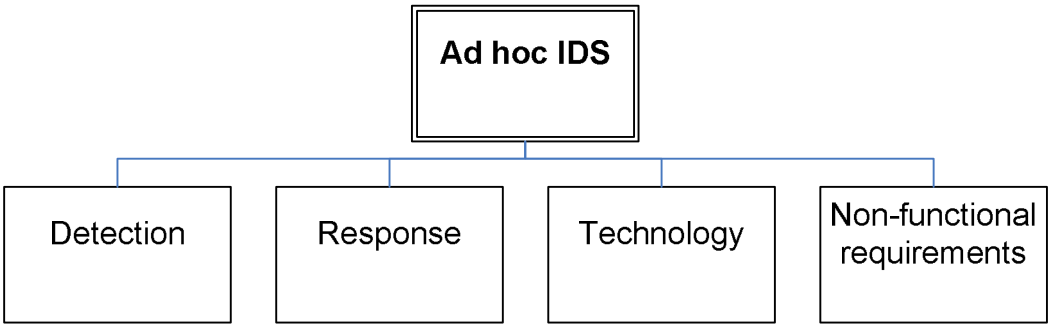

Figure 3. Requirements structure.

Detection

- The IDS shall be able to detect previously known and unknown attacks on all network layers.
- The IDS shall also be able to detect and identify malicious nodes.
- Detection shall be performed in close to real-time.

Response

- The response shall be automatic.
- The response shall take effect within a few minutes from detection.

Technology

- Distributed solution
- Autonomous
- Survivability
- Economy

Non-functional requirements

- Not introduce new weaknesses
- Reliable

4 IDS architecture

This section proposes a node-based network IDS architecture, with some coordination performed by a central server.

4.1 Limitations and scope

Before presenting the proposed architecture some interpretations of the requirements earlier stated is in order.

To reduce the risk of spoofing a node has to provide proof of identity. By doing so, a receiving node has the ability to verify the claimant identity through the identification system. How this is done is outside the scope of this report. If a node fails to provide proof of identity, or the identity is false, the receiving node alerts the central server which in turn can initiate a response.

The receiving node itself may be under the control of an enemy. The IDS does not provide any control of outgoing traffic from the node. It is up to receiving nodes to discover compromised or enemy nodes.

In the section of military requirements the requirement for radio silence is not considered in this report, since it is more of an implementation issue rather than a design issue.

As mentioned earlier when talking about decentralized infrastructures, a fully decentralized solution requires collaborations between nodes. The current level of collaborating protocols within the research community is not secure enough for nodes to work together. The general requirement for not introducing new vulnerabilities is given a higher priority, thus prohibits nodes from collaborating in security issues.

4.2 Network layers and operating system

First, let us recall the traditional four layers of the TCP/IP-stack. From the bottom and up (see Figure 4), the nodes are connected with a channel that delivers raw data transmitted by a modulated signal. A node receives (and transmits) the modulated packet with a Network Interface Card (NIC), and promotes it to the Link layer. The stack removes the outermost link header and in the case of the Internet Protocol (IP) promotes it to the Network Layer. Then the IP header is stripped, and the packet becomes promoted to the Transport layer, which is either Transport Control Protocol (TCP) or User Datagram Protocol (UDP). The packet reaches the application through the socket layer, secure socket layer (SSL), or some other application interface.

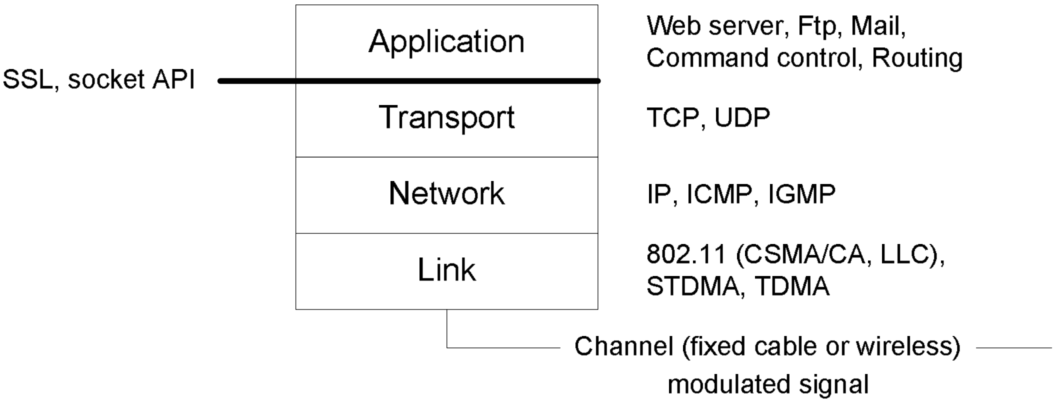
Application
Transport
Network
Link
SSL, socket API
Web server, Ftp, Mail, Command control, Routing
TCP, UDP
IP, ICMP, IGMP
802.11 (CSMA/CA, LLC), STDMA, TDMA
Channel (fixed cable or wireless)
modulated signal

Figure 4. Layers of the TCP/IP stack.

The four layers are of utter importance for the architecture, since each layer may use its own method of encryption, thus making it difficult to monitor the payload in each packet. The stack also represents the order of how an attack has to work itself through a node.

It is of interest for the IDS to intercept traffic before it reaches its intended application. Figure 5 is a simplified picture of what happens when a packet comes into a node for a Linux system. The stack must decide if the packet should be bridged (forward by link layer) or routed (forwarded by network layer) to another node, or if the packet is designated for the local node (local processing). There are in the picture five tap-points called hooks (circular objects), where it is possible to steal or monitor the packet by an external program. A description of how this can work in windows can be found in (Windows Filtering Platform).

For the three cases of packet flows mentioned, it is possible to intercept them before anything is done with the packet (pre-routing) or after everything has been done to it (post-routing). In this architecture the focus is not on packets being bridged, routed or outgoing since it does not harm the local node. However, packets that are addressed to the receiving node are equivalent to the input hook. This is where the traffic should be intercepted in the IDS architecture.

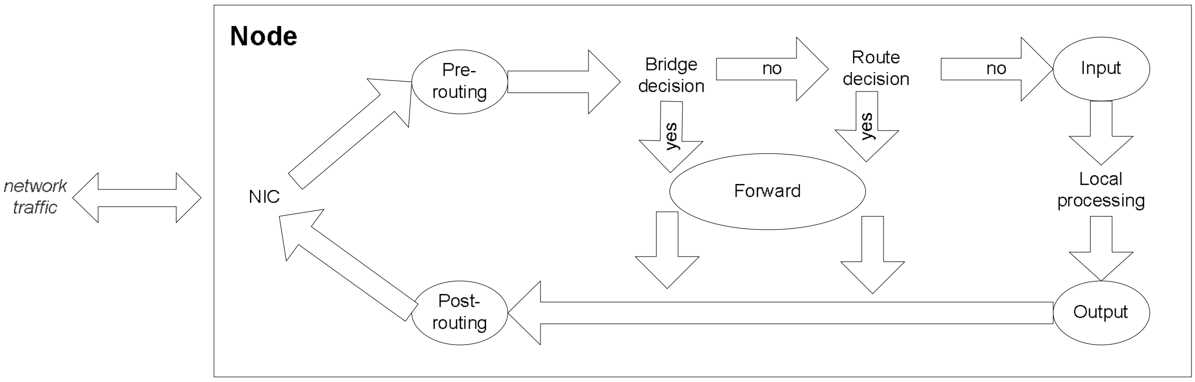

Figure 5. Hooks in link and network layer processing of packets inside a node.

4.3 Central server and response

The nodes do not cooperate with help of any distributed detection algorithm; the detection is strictly performed on local basis. When a central node is within reach, a node will report its findings and perform software synchronization. The reach could be direct or indirect via caching in or routed through neighbouring nodes, see Figure 6. When communicating status, software, configurations etc., the identity of the source is especially important to avoid alteration from an enemy node.

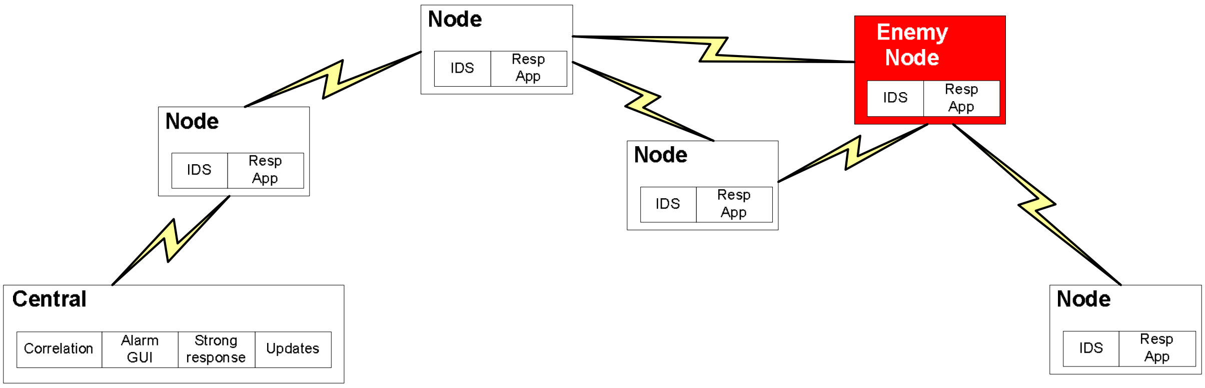

Figure 6. Tactical mobile ad hoc network with a centralized server.

Automation is a key issue on a local level. The user should not be forced to administrate the IDS configuration, although there may be situations where this is necessary. As a default the IDS should be set to automatically apply weak responses. It is however possible for a user to conduct a manual response but this response still categorizes under weak responses.

All status is forwarded to the central server, where alarms are displayed in a graphical user interface (GUI) to the administrator. The administrator can then choose to perform a strong response, which is manually triggered. The strong response will communicate with the response application residing on each node. Updates (like new rules, software versions, etc.) are pushed to the distributed IDS nodes.

The worst attack is when a node gets infiltrated, since the enemy gain access to valid keys and thus can commit an attack within the system.

4.4 Node components

Figure 7 shows the dataflow inside a node, and how the (same) IDS module is invoked from different points in the flow to access all traffic to achieve the best result. The components differing from an installation of a common operating system is described below.

In this subchapter the architectural components surrounding the IDS is presented. The actual IDS module is presented in the next subchapter.

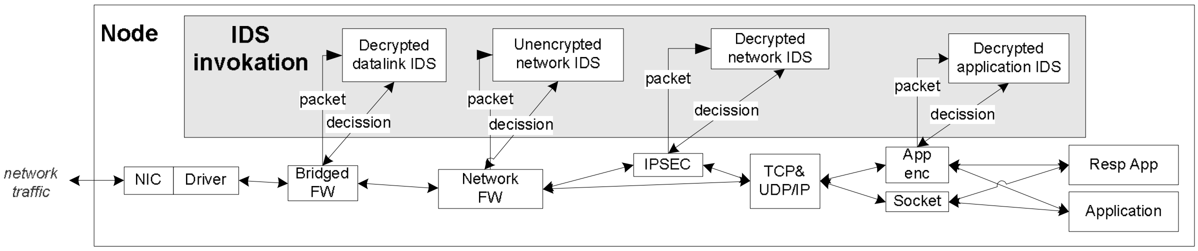

Figure 7. Network traffic flow and hooks for IDS inside a node.

4.4.1 Network Interface Card (NIC) and driver

The NIC and network driver receives and transmits data from and to other nodes. The link layer encryption and decryption is also performed here. Inner modules are not affected by this encryption.

4.4.2 Firewalls

The architecture incorporates two firewalls in order to cover more layers. The first one protects the link layer, called bridged firewall. The second is a more traditional firewall and it covers the other layers.

The precise operating system in use should not matter. Comparisons with this architecture have been made for Win2000/XP and Linux. Both seem to provide some hooks that are necessary for real-time IDS to make decisions on incoming traffic. However, the concept of a bridged firewall has only been found in Linux, and there are many more hooks defined in its network code.

Bridged firewall

The bridged firewall receives data from, and sends data to the NIC. In Linux, this is typically Ebtables, see (Ebtables).

Network firewall

The network firewall is equivalent to a regular firewall. It guards the network and upper layers, protecting them from attacks. It contains filtering capabilities for IP, TCP and UDP. To analyze application data, plug-ins is needed. In Linux the firewall is usually IPtables, see (Netfilter), and applications are supported with connection tracking.

4.4.3 IPsec decryption

IPsec is tightly connected with the TCP/IP stack. There are two alternatives to intercept the traffic:

- Use hooks provided by IPsec or TCP/IP.
- Modify the source code of IPsec or TCP/IP

Modifying source code is easier in Linux compared to Microsoft Windows simply because the source code for Linux application is made available. A modification of Windows requires some cooperation by Microsoft.

4.4.4 Application decryption

Military applications may use some encryption. Applications for the operating system are likely to use the default encryption shipped with it. Other applications could use proprietary encryption libraries. For the IDS to inspect the encrypted payload for all applications, hooks must be inserted in the encryption libraries or in the applications.

Military applications are most likely to use multicast for distribution of message text, situation awareness, audio, and video. Multicast uses UDP, and the encryption could be S-MIME.

More common applications like web servers and java often use their own version of SSL (Secure Socket Library). There can be many different implementations of SSL running in a system simultaneously.

4.4.5 Response application

The response application can inform a central server about the status, and reconfigure applications to perform automatic weak response. It also receives updates and orders about strong response (e.g. force the current user to re-authorize) from the central server.

4.5 The IDS module

For the IDS to work properly, it has to be able to investigate the payload of the packets traversing the node. How a packet is encrypted has great consequences on how the IDS can investigate it.

The IDS module in the proposed architecture can be invoked several times depending on how a packet is encrypted. In the worst case, when a packet is encrypted both with IPsec and SSL, the IDS module is invoked four times (see Figure 7). In this case the network firewall associated with the IDS is only able to see the encrypted packet when trying to examine the IPsec and SSL payload.

It is basically the same IDS module that is invoked every time. Depending on from where the invocation is made, the IDS can investigate different packets. There are four invocations points defined; all except decrypted datalink will try to cover all unencrypted layers above it, since these will otherwise be missed:

- Decrypted datalink (will not investigate packet for network layer and up)
- Unencrypted network (also unencrypted transport and application)
- Decrypted network (also unencrypted transport and application)
- Decrypted application

Since the traffic flow is halted for each investigation by the IDS, it is of utter importance that the packet analysis is performed in real-time. The set of rules for each detector should be kept to a minimum.

Anomaly based detectors requires heavy processing and generates too many false alarms to be of interest for a tactical mobile network. Specification based detectors have a very good detection rate and generates few false alarms. Both known and unknown attacks can be covered by the specification. It can be a problem for engineers to generate the needed specifications in acceptable time, and the specifications must probably be updated whenever changing the software. If this cannot be done immediately, a backup solution is to have an additional signature-based detector to catch known attacks. Figure 8 gives an overview of the IDS module.

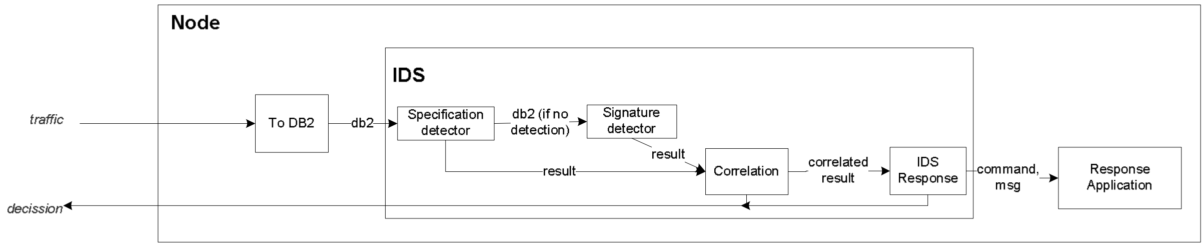

Figure 8. Overview of IDS module.

4.5.1 Specification-based detector

The specification-based detector needs specification rules for link layer protocols (like ARP, MAC, CSMA/CA), network layer protocols (IP and routing), transport layer protocols (UDP, TCP) and application layer protocols (routing, military applications). Attacks towards routing should be relatively easy to detect since the sender must sign its message and cannot fake from where it was sent (which makes spoofing impossible), see (Hansson, Nordqvist & Persson, 2005).

The specification based detector applies its rules first and, if nothing is found, the signature-based detector is also invoked, see Figure 8.

4.5.2 Signature-based detector

A signature-based detector is suggested as the backup detector. Rules that apply should be tested only once to avoid unnecessary computing.

Figure 8 shows the deployment and dataflow of the two detectors which are applied on incoming traffic. The specification based-detector is first invoked, and only if it does not find anything the signature-based detector is invoked.

4.5.3 Correlation and IDS Response module

The correlation module collects alarms from the detectors, and notifies the IDS response module if a threshold is reached, otherwise it informs the firewall or decryption module to let the packet pass. The IDS response module decides appropriate action and can either tell the firewall or decrypting software to drop the packet or notify the Response application about a desired action.

4.6 The architecture and the requirements

This subchapter compares the proposed architecture with the requirement listed in subchapter 2.2.

4.6.1 General requirements

GR01 Automatic detection

The IDS detection modules (specification-based and signature-based) detect intrusions without the cooperation and involvements of an administrator or user.

GR02 Powerful automatic response

The local response acts without the use of human control.

GR03 Fault-tolerant and attack resistant

The specification-based detector operates in such way that deviation from the intended use is discovered.

GR04 Only system administrator may configure and modify the system

Locally the IDS is user-independent.

GR05 Transparency

The user does not take active part in the operation of the IDS, thus the IDS operates independent of the user.

GR06 Low false rate, high detection rate

The specification-based detector has been shown reliable in tests.

GR07 Not introduce new weaknesses

Since the IDS do not involve cooperation between nodes, it does not open up itself to new weaknesses found in distributed protocols.

GR08 Scalable

The system is scalable since there are no dependencies between the nodes. Arguably, the central server for the strong response could become a bottleneck but since the system does not need to be in constant contact with the server it does not become a problem.

4.6.2 Specific requirements

SR01 Autonomous

The ad hoc approach itself provide for operation in an environment where the infrastructure is under developed or destroyed.

SR02 Economy

The communication overhead within the network is not much affected by the IDS since the nodes do not communicate with each other. The burden the specification-based and the signature-based detector places on the node internally is based on the amount of rules the specification contains. Thus it is both a question of how well the specification file and the signature file is written as well as how they are maintained.

SR03 Detect attacks on all layers

The architecture is layered thus able to detect attacks on all layers.

SR04 Identify malicious nodes

If authentication is enforced, an attacking node will compromise itself as soon as a message is sent that deviate from what the specification specifies. With the use of authentication, it is possible for a node to detect witch node is malicious an either counter with a weak response or a strong response.

4.6.3 Military requirements

MR01 Automatic response

The local (weak) response is an autonomous action. The same goes for the communication with the central server. The system do not wait for an operator to initiate a response, something that would only slow the process down (the operator may by preoccupied with other duties). How fast a response should be put into action is a matter of configuration and thus a policy decision.

MR02 Attack detection

The specification-based detector should be able to detect unknown attacks. Any deviation from the written specification, whether it is slight or obvious, should result in a response.

MR03 Distributed protocols

The IDS is not dependant on any central function. Responses from the central server in the architecture is optional, hence the system is in no way dependant of being in continuously contact with the central server.

MR04 Survivability

Being node based, the IDS is only dependant of power supply from the host. Hence, the surrounding environment poses no restrictions on the IDS capability to operate. Also, the detection methods used by the IDS operates autonomously, thus are able to operate under poor network conditions.

MR05 Radio silence

The ability to hinder the IDS to communicate is one of the few modes the operator is allowed to control. The IDS should be implemented in such way that it is possible to configure a stealth mode (i.e. listen only) when radio silence is ordered. Radio silence is thus more of an implementation issue than an architectural requirement.

5 Future work

The work with an IDS for a mobile ad hoc network has thus far been limited to a theoretical study.

One of the parameters for the trilateral project was to see if the suggested architectures for IDS, boundary protection and authentication could be accomplished with commercial-off-the-shelf technology. Therefore, one possible continuation is to prototype an IDS based on, for instance, Snort Wireless. This would provide insights if it is at all possible to modify an existing IDS tool to be operable in a mobile ad hoc network.

The proposed IDS architecture requires a few issues to be solved before it can operate properly. Issues like secure communication with the central node for status reports and software updates, a unique identity for each node, local security in the node so that the integrity of configuration and data is maintained, are just examples of what is needed to be looked into before an operational IDS is feasible. An interesting proposal for future work would be to try to integrate the proposed architectures from each member in the project.

6 References

6.1 Documents and papers

Carlinet, Y. et al.: "Response Requirements Specification", DIADEM Technical Report D4, July 2004
Available via http://www.diadem-firewall.org/documents, last visited June 28. 2005

Kossakowski, K. et al.: “Responding to intrusions”, Carneige Mellon Software Engineering Institute, February, 1999

Hansson, E., Grönkvist, J. & Nilsson, J.: Intrångsdetektering i mobila ad hoc-nät, FOI-R--1375--SE, November 2004

Hansson, E., Nordqvist, D. & Persson, K.: Specification-based intrusion detection for mobile ad hoc networks, 2005 but not yet published.

Hansson, E. & Hansson, A.: Evaluation of wireless Intrusion Detection tools for Mobile Ad Hoc Networks – Evaluation, Threats Analysis and Typical Cases, FOI-R--1374--SE, November, 2004

Hawrylkiw, D.: “Intrusion Detection FAQ: Network Intrusion and use of Automated Responses”, SANS Institute
Available via http://www.sans.org/resources/idfaq/auto_res.php, last visited June 28, 2005

Ko, C., Fink, G. & Lewitt, K:. Automated Detection of Vulnerabilitites in Privileged Programs by Execution Monitoring, In Proceedings of the 10th Computer Security Application Conference, Orlando, Florida, December 5-9, 1994

Kumar, S.: Classification and Detection of Computer Intrusions, PhD thesis, Purdue University, 1995

Kumar, S. & Spafford E.: A Pattern Matching Model for Misuse Intrusion Detection, In Proceedings of the National Computer Security Conference, Baltimore, 1994

Larsen, J. & Haile, J.: “Understanding IDS Active Response Mechanism”, January, 2002
Available via http://www.securityfocus.com/infocus/1540, last visited June 28, 2005

Mishra, A., Nadkarni, K. & Patcha, A.; “Intrusion Detection in Wireless Ad Hoc Networks”, IEEE Wireless Communications, February, 2004

Project arrangement number 2004-03 to the CA/NL/SW cooperative science and technology memoranding of understanding, 28 May 2003, concerning Secure Mobile Ad hoc Networks, FOI Dnr 04-1001:5

Uppuluri, P. & Sekar, R.: Experiences with Specification-Based Intrusion Detection, Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection, Davis, CA, October 10-12, 2001

Zhang, Y. & Lee, W.: “Intrusion detection in wireless Ad Hoc Networks”, 6th Int’l. Conf. Mobile Comp. and Net., August, 2000, pp.275-283

6.2 www references

Snort

http://snort-inline.sourceforge.net/, last visited April 1, 2005

Ebtables

http://ebtables.sourceforge.net/, last visited April 24, 2005

Netfilter

http://www.netfilter.org/, last visited April 24, 2005

Windows Filtering Platform

http://www.microsoft.com/whdc/device/network/WFP.mspx, last visited June 27, 2005