ESPOO 2005 VTT PUBLICATIONS 580

Kaarina Karppinen

# Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment

VTT PUBLICATIONS 580

# Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment

Kaarina Karppinen

VTT Electronics

ISBN 951–38–6671–8 (soft back ed.)
ISSN 1235–0621 (soft back ed.)

ISBN 951–38–6672–6 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0849 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde 020 722 111, faksi 020 722 4374

VTT, Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel 020 722 111, fax 020 722 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O.Box 2000, FI–02044 VTT, Finland
phone internat. +358 20 722 111, fax + 358 20 722 4374

VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU
puh. vaihde 020 722 111, faksi 020 722 2320

VTT Elektronik, Kaitoväylä 1, PB 1100, 90571 ULEÅBORG
tel. växel 020 722 111, fax 020 722 2320

VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FI–90571 OULU, Finland
phone internat. +358 20 722 111, fax +358 20 722 2320

Technical editing Anni Kääriäinen

Valopaino Oy, Helsinki 2005

Karppinen, Kaarina. Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment [Hyökkäyspuihin perustuva tietoturvan mittaaminen liikkuvassa spontaanissa (Ad Hoc) verkkoympäristössä]. Espoo 2005. VTT Publications 580. 57 p. + app. 8 p.

**Keywords** security measurement, attack trees, mobile ad hoc networks, network protocols, network security, mobile internet protocol, data transfer, vulnerability, evaluation

# Abstract

Practical evidence of the actual security performance of network systems is needed in order to be able to manage them in an adequate way.

This study investigates whether the attack tree approach can be used for identification of the appropriate data to be measured in a mobile ad hoc network environment, and whether divergent results of attack tree analysis are obtained with different types of network protocols. The study focuses on the data transmitted in the network in connection with attacks against the Ad hoc On-demand Distance Vector protocol (AODV) and Mobile Internet Protocol version 6 (MIPv6). The network type and the protocols used in this study were chosen because of their novelty and their potential importance in future communication scenarios.

Based on the results of the study, the attack tree approach is a helpful systematic method for exploring vulnerabilities. However, it is not suitable for a very detailed analysis of the attacks in the area of network protocols when applied manually. This is due to the complexity and diversity of information networks, which causes attack trees to inevitably grow uncontrollably large. Furthermore, this study shows that the results obtained by applying attack tree analyses differ depending on the protocol.

Karppinen, Kaarina. Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment [Hyökkäyspuihin perustuva tietoturvan mittaaminen liikkuvassa spontaanissa (Ad Hoc) verkkoympäristössä]. Espoo 2005. VTT Publications 580. 57 s. + liitt. 8 s.

**Avainsanat** security measurement, attack trees, mobile ad hoc networks, network protocols, network security, mobile internet protocol, data transfer, vulnerability, evaluation

# Tiivistelmä

Konkreettisia todisteita tietoverkkojen todellisesta turvallisuudesta tarvitaan, jotta tietoverkkoja voidaan hallita oikealla tavalla.

Tämä tutkimus pyrkii selvittämään, voidaanko hyökkäyspuumallia käyttää hyväksi soveliaan mitattavan tiedon määrittämiseen liikkuvassa spontaanissa (ad hoc) verkkoympäristössä ja saadaanko erityyppisillä verkkoprotokollilla toisistaan poikkeavia tuloksia hyökkäyspuutulosten analysoinnissa. Tutkimus keskittyy Ad hoc On-demand Distance Vector- (AODV) ja Mobile Internet Protocol version 6 (MIPv6) -protokolliin kohdistuvien hyökkäysten aikana verkossa kulkevaan dataan. Tutkimuksessa käytettävä verkkotyyppi ja verkkoprotokollat valittiin niiden uutuusarvon perusteella ja siksi, että niiden oletetaan olevan tärkeitä tulevaisuuden tietoliikenteessä.

Tutkimustulosten perusteella hyökkäyspuumalli on hyödyllinen menetelmä haavoittuvuuksien tutkimiseen. Manuaalisesti tehtynä se ei kuitenkaan sellaisenaan sovellu hyvin erittäin yksityiskohtaiseen verkkoprotokolla-alueen hyökkäysten analysointiin, koska tietoverkot ovat niin monimuotoisia ja kompleksisia, että hyökkäyspuut kasvavat väistämättä hallitsemattoman suuriksi. Tutkimuksessa havaittiin myös, että hyökkäyspuuanalyysin tulokset olivat erilaisia tutkimuksen kohteena olevasta verkkoprotokollasta riippuen.

# Preface

*"Either I will find a way, or I will make one."*
– Sir Philip Sidney (1554–1586)

This study was completed within the VTT, Technical Research Center of Finland, Electronics, Software Architectures group, Security team. The study was funded by the strategic theme projects TRUST and MMAUTO at VTT Electronics in Oulu, Finland, during 2005.

I would like to thank all the people who contributed to this master's thesis. First of all, my supervisors, Mr. Jorma Kajava of the University of Oulu and Mr. Reijo Savola of VTT; thank you for the valuable conversations and guidance. I similarly wish to thank Professor Petri Pulli of the University of Oulu for commenting on this work. Also, my team colleagues: Mr. Pasi Ahonen, Mr. Jarkko Holappa, Mr. Mikko Rapeli, Ms. Anni Sademies, Mr. Ilkka Uusitalo and Mr. Timo Wiander; thank you for giving me advice and support and for keeping my spirits up throughout the whole process. Furthermore, Mr. Jouko Sankala of Nethawk, thank you for your interest in my research and the valuable discussions concerning network measurements in practice.

Special thanks to the Maceketeers, for your continuous encouragement and faith in me during my studies. Finally, my family: I wish to express my deepest love and gratitude to Mika, Aki and Miska for supporting me endlessly and giving me the possibility to concentrate on my studies. I truly appreciate that with all my heart.

Lämpimimmät kiitokseni myös Asta ja Olavi Karppiselle. Ilman teidän kannustustanne ja konkreettista apuanne opintoni eivät mitenkään olisi onnistuneet tätä tahtia.

In Oulu, Finland, 31st August, 2005

Kaarina Karppinen

# Contents

# Terms and Abbreviations

| | |
|---|---|
| AH | Authentication Header; provides authentication of the sender and of data integrity |
| AODV | Ad hoc On-demand Distance Vector protocol; an algorithm for routing data across ad hoc networks |
| BU | Binding Update; a procedure whereby the mobile node informs HA or CN about its new CoA |
| CC | Common Criteria for Information Technology Security Evaluation; an international standard (ISO 15408) for computer security |
| CN | Correspondent Node; a node that communicates with a mobile node |
| CoA | Care-of-Address; a temporary address used by a mobile node while it is attached to a foreign link |
| DoS | Denial of Service attack; purpose is to prohibit an opponent from using a program or an entire system |
| DDoS | Distributed Denial of Service attack; a DoS attack by several co-operating attackers |
| ESP | Encapsulating Security Payload; provides data integrity, data confidentiality and authentication |
| HA | Home Agent; a router on a mobile node's home network that tunnels packets to the mobile node while it is away from home |
| HoA | Home Address; a mobile node's IP address that remains unchanged regardless of where the node is attached to the Internet |
| IETF | Internet Engineering Task Force; open community for engineers, scientists, vendors, operators, etc., that facilitates discussions and standards for the Internet |

| | |
|---|---|
| IDS | Intrusion Detection System; a tool used to detect unauthorised access to a computer system or network |
| IP | Internet Protocol; a standard that allows the transmission of data across networks |
| IPS | Intrusion Prevention System; an access control tool used to prevent unauthorised access to a computer system or network |
| IPsec | Internet Protocol Security; standard suite of protocols for network-layer confidentiality and authentication of IP packets |
| IPv4 | Internet Protocol version 4; a current version of IP that supports a 32-bit address space |
| IPv6 | Internet Protocol version 6; a new version of IP that supports a 128-bit address space |
| ISO | International Organization for Standardization; a worldwide federation of national standards bodies |
| MANET | Mobile Ad hoc Network; self-organising network of mobile routers connected by wireless links |
| Measuring point | Part of the protocol frame, a triplet consisting of the data itself, the specific time and the specific direction of the data |
| MiM | Man-in-the-Middle attack; purpose is to listen to the messages between two parties and possibly also modify, delete, and replay the messages |
| MIPv6 | Mobile Internet Protocol version 6; a version of the IPv6 standard where a mobile node is always identified by its home address, regardless of its current point of attachment to the Internet |
| MN | Mobile Node; a node that can change its point of attachment from one network or subnet to another |
| NAT | Network Address Translation |
| Node | Device that is directly connected to the network |

PDA Personal Digital Assistant; a handheld computer or personal organiser device

RERR Route Error message; AODV protocol message that indicates the unreachable destinations in MANET

RFC Request for Comments; Internet standards-related specifications and working notes of the IETF

RR Return Routability; a procedure to provide proof that the mobile node is reachable at both its HoA and its CoA

RREP Route Reply message; AODV protocol message unicasted to inform about a requested route in MANET

RREP-ACK Route Reply Acknowledgement message; AODV protocol message unicasted to acknowledge a route reply in MANET

RREQ Route Request message; AODV protocol message broadcasted to find a route in MANET

SSE-CMM Systems Security Engineering Capability Maturity Model; a process reference model to improve and assess the capability of security engineering

Tiger team Group or organisation that conducts penetration testing by attempting remote attacks via networks or other communication channels in order to assess the security of computer systems

TCP/IP Transmission Control Protocol/Internet Protocol; a suite of communication protocols used in the Internet and other networks

# 1. Introduction

Our society is becoming more and more dependent on communication networks. Mobile ad hoc networks (MANETs) have great potential for broad use in making ubiquitous computing applications possible and successful because they enable self-organisation and dynamic operation in a network. Information security is commonly agreed to be vital in today's networked environment. However, stating that a certain network is secure is still a difficult task. More facts about a network's security, or insecurity, could be stated by measuring some predefined attributes of the network and comparing the measurement results with a certain predefined baseline.

The aim of this study is to investigate whether MANET security can be measured with the help of attack trees (Schneier 2000, 318–333). The approach is analytical and technical, based on the Ad hoc On-demand Distance Vector (AODV) (Perkins et al. 2003) and Mobile Internet Protocol version 6 (MIPv6) (Johnson et al. 2004) network protocols. The primary objective of this study is to gain experience in the use of attack trees for the development of metrics for measuring information security in networks. This is done by focusing on the data transmitted in the network in connection with example attacks against MANETs. That data is analysed in order to detect and prevent attacks by finding the parameters to be measured.

Information security is a wide area and includes a lot more than analysing, detecting and preventing attacks against the network. This study is limited to intentional attacks against one type of network. It must be remembered that the security of the whole system cannot be defined solely by the number of attacks against it. This study only covers a small part of the big picture.

The theoretical basis of this study is formed by a literature analysis. The main references in the literature study have been The Internet Engineering Task Force's (IETF's) working groups and Request for Comments (RFCs), Savola (2005) and Schneier (2000, 318–333). The gathered background information is used as a basis for attack tree analyses, which assist in identifying the appropriate data for measuring. Identification is needed for security metrics heuristic development as well as for developing the attack tree analysis further.

This research path is shown in Figure 1, where the potential development of the results of the study is marked with white shapes.

The motivation for this study arises from the need to obtain evidence on the actual security performance of network systems. More information about and concrete methods for network security measurement are needed and the results of this study are expected to be valuable for a number of measurement applications. The attack tree approach has not previously been used in this context and this study may be opening new doors and dimensions within MANET security research, and the research on security metrics as well.

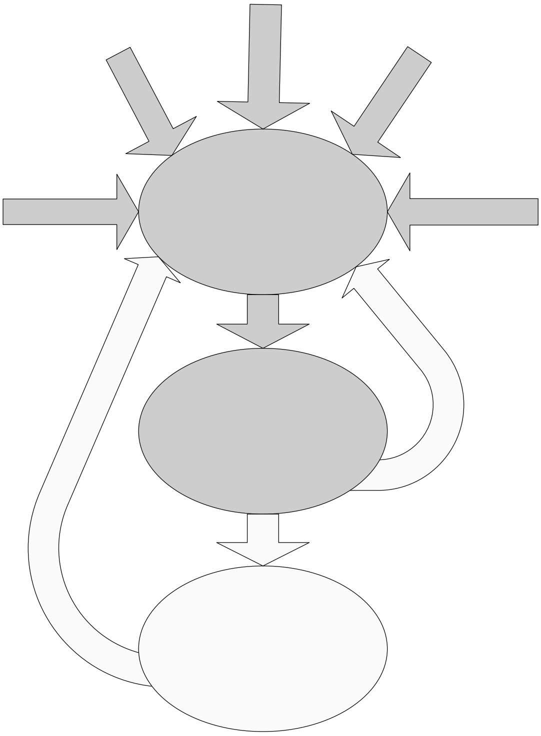


*Figure 1. Research path used in this study.*

The main goal of this study is to answer the following research problem:

- "Can attack trees be utilised for identification of the appropriate data to be measured in order to obtain evidence of the actual security performance of a mobile ad hoc network?"

The subgoal of this study is to answer the following question:

- "Do the results of attack tree analysis differ depending on the protocol?"

These questions are answered by the construction of example attack trees and an analytical investigation. Case examples of the attacks against MANET are defined, their attack trees are constructed, and the results of those examples are analysed. The novelty of this study lies both in the information security measurement aspect, which has not been researched very much, and the use of attack tree analysis in a network protocol context. The protocols in question have been selected so that they act in different network layers and the results could give a wider perspective on the problems. The apparent future importance of these protocols has also influenced their selection.

The remainder of this document is organised as follows: Chapter 2 overviews the background of MANETs, and the AODV and MIPv6 protocols. Chapter 3 presents the basis for network security and measuring it. In Chapter 4 the focus is on the attack trees; practical examples of attacks and their attack trees are presented. The attack tree examples are analysed and the results of the analyses are given in Chapter 5. In Chapter 6 the results, their value and their limitations are discussed and some future research questions are raised. Final remarks in Chapter 7 close the study. The message formats and fields of AODV routing messages and MIPv6 packages are shown in Appendix A and Appendix B respectively.

# 2. Mobile Ad Hoc Networks and Network Protocols

This chapter presents the background information related to the mobile ad hoc networks and the protocols used in transferring information in them. First, the basic characteristics that distinguish MANETs from other networks, as well as the attack types that threaten them especially are introduced. After this, the network protocols examined in this study are overviewed.

## 2.1 Mobile Ad Hoc Networks

MANETs fundamentally differ from traditional wireless mobile networks because they do not rely on any fixed infrastructure such as base stations or mobile switching centres. Nodes have the ability to self-organise dynamically, and control and management of the network is distributed among the nodes. There are no routers as all the nodes are responsible for routing the data. MANETs can also be of various forms and sizes. The number of nodes in a MANET may range from two to thousands and the devices within a MANET can be of different types, sizes and capabilities. There are a variety of different mobile devices that are being used more and more pervasively in various networks. At the lowest capacity level in terms of computing power are special-purpose devices (for example, different sensors) and mobile phones. More powerful, general-purpose mobile devices are generally termed Personal Digital Assistants (PDAs). At the highest capacity level in terms of computing power are computers, laptops or others. All these devices can be used in MANETs as long as they fulfil the minimum requirements, such as being able to act as a router in a network.

MANETs can be used to provide network facilities easily and rapidly, when and where needed, especially in places and situations where it isn’t possible or cost effective to form a fixed network. MANETs only need minimum setup requirements, so they can be deployed with relatively low installation, maintenance and administration costs. Nodes can join the network on-the-fly and share information and resources based on their needs, even if the wired infrastructure is inaccessible, overloaded, damaged or destroyed. For all these reasons, the interest towards them has increased noticeably during recent years.

As the technology of MANETs has matured over the last few years, the research emphasis has changed to the security issues in them. Thus their security concerns are still far from solved. The attack types threatening MANETs in particular, and their explanations, are shown in Table 1.

*Table 1. The most common types of attack against MANET.*

| Attack | Explanation |
|---|---|
| Black hole | Black hole attack has two phases. First an attacker gets all traffic in the network or to a certain node to flow via itself by advertising false routing information. Then it can simply drop some or all of the packets it was supposed to forward. |
| Denial of Service | Denial of Service (DoS) attack means preventing authorised users from accessing services offered by the network. Black hole attack and resource consumption attack are practical examples of a DoS attack. An even more severe form of the DoS attack is the distributed DoS (DDoS) attack, where a group of attackers work together in preventing authorised users from accessing the network services. |
| Eavesdropping | Eavesdropping is a passive attack. An attacker listens to the network and routing traffic and attempts to discover the nodes' information. Detection of passive attacks in wireless networks is usually impossible but network nodes are generally able to protect their data by encryption and thus prevent eavesdroppers from getting any valuable information. However, especially in MANETs, not all the nodes have sufficient resources to carry out the authentication and encryption procedures. |
| Impersonation, Man-in-the-Middle | Impersonation attack means that an attacker takes the identity and privileges of a trusted node. One type of impersonation attack is a man-in-the-middle attack (MiM), where an attacker reads and possibly modifies messages between two nodes, so that neither of the end nodes knows that they have been attacked. |
| Physical attack | Physical attack means device tampering, where a device is physically harmed, damaged, captured or stolen. Mobile devices are especially vulnerable to this kind of attack because of their portable size and nature. |
| Resource Consumption | Resource consumption, also known as sleep deprivation torture, attack means that an attacker tries to wear out the network's |

| | |
|---|---|
| | resources and/or the nodes in it. For example, these attacks can be in the form of unnecessary requests for routes, injecting a large number of unnecessary packets into the network, or forwarding unnecessary packets to nodes. MANET nodes in general have limited resources of bandwidth, battery and computational power. Power exhaustion attacks in MANETs are a real, powerful threat because a node can no longer function in the network once its battery runs out. |
| Wormhole | Wormhole attack means that an attacker selectively tunnels packets from one place in the network to another. Wormhole is the tunnel between the two attackers, which are linked via a private network connection. Due to MANETs' shared broadcast radio channel, the attacker can create a wormhole for packets addressed to any node in the network. |

Even though MANETs' basic characteristics have significant advantages over a typical wireless infrastructural network, they also substantially complicate the security issues. Some of the basic MANET characteristics that cause difficulties in providing security in MANETs include lack of central authority, lack of association among nodes, shared broadcast radio channel, and physical vulnerability. Nodes in a MANET can move randomly and thus the network topology can change frequently and unpredictably. The fact that the nodes are capable of routing is a source of new kinds of security threats. Maintaining and updating the routing tables is a task in which a malicious node can do a lot of harm. Furthermore, as each node in a MANET is acting as an end user system and a router at the same time, additional energy is required to forward packets from other nodes. This causes limitations to services and applications due to the nodes' limited processing power and availability of resources. In practice, for example, the use of encryption algorithms can consume so much in the way of resources that it is not a realistic option for some nodes.

## 2.2 Network Protocols

A protocol is an agreement between the communicating parties on how the communication is to proceed (Tanenbaum 1996, 17). Most network implementations are organised as a series of layers, each one built upon the one below it. Every layer has its own set of protocols. MANETs are most often designed to follow the TCP/IP (Transmission Control Protocol/Internet Protocol) network architecture.

### 2.2.1 Ad-Hoc On-Demand Distance Vector Protocol

The Ad hoc On-demand Distance Vector (AODV) protocol is a reactive routing protocol that uses packet exchanges to establish routes. It is an application layer protocol that exchanges routing messages between nodes and maintains routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Routes are determined on-demand when needed, that is only when there are data packets to send and the route to the destination node is not known. AODV is a widely used routing protocol within MANETs. It is quick and offers reliable loop-free routing. AODV's desirable features also include quick adaptation to dynamic link conditions, low processing and memory overhead, and low network utilisation. (Perkins et al. 2003.)

AODV has three basic types of routing messages: Route Requests (RREQ), Route Replies (RREP), and Route Errors (RERR). In addition, a Route Reply Acknowledgement (RREP-ACK) message is sometimes used to acknowledge receipt of an RREP message. Though not required, AODV may utilise a "Hello" message to maintain the local connectivity of a node. AODV is a stateless protocol; the node updates its routing table every time it forwards or receives an RREP message. Figure 2 shows four examples of message exchanges using the AODV protocol.

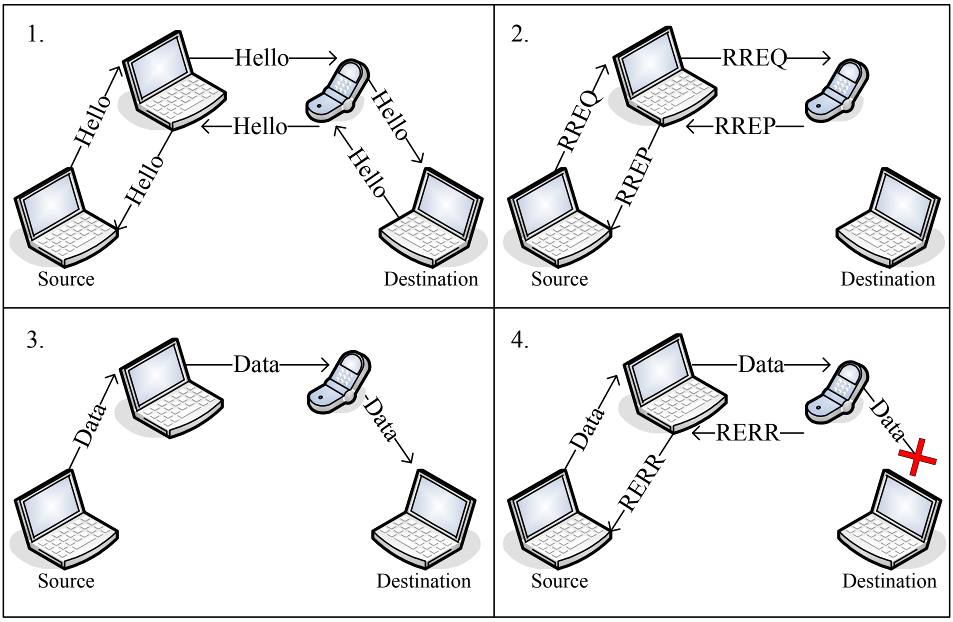


*Figure 2. AODV protocol messaging examples.*

The first example shows transmission of "Hello" messages through the network. The second example shows the basic procedure for finding the appropriate route. When a source node wants to send packets to a destination node and does not have a valid route in its routing table, it will broadcast an RREQ. If the intermediate node has an active route to the requested destination, it will unicast an RREP back to the source node. Otherwise, the RREQ will be re-broadcast further. Because multiple paths may exist between two nodes, a node can receive the same RREQ more than once. The third example shows the situation after the route has been found and the data packets are transferred. The nodes also send out RERR packets to report broken paths and activate the route re-discovery procedure. The fourth example shows the situation where an intermediate node notices that the route is no longer valid.

AODV is a potential protocol for widespread standardisation, despite its total lack of security features. As stated by Perkins et al. (2003), AODV is designed for use in networks where the nodes can all trust each other, either by the use of preconfigured keys or because it is known that there are no malicious intruder nodes. They also state that in the cases where no such trust exists it is wise to protect AODV control messages by authentication techniques such as IP security (IPsec) (Kent & Atkinson 1998) when applicable. Enhanced protocols based on AODV with added security features have been developed but they are not as commonly used as basic AODV, partly because all the security features come with the cost of increased resource consumption, which means reduced efficiency. The formats of AODV routing messages are further explained in Appendix A.

## 2.3 Mobile Internet Protocol Version 6

Internet Protocol (IP) is a network layer protocol that ensures that the devices in different networks are able to communicate with each other and that data packets are addressed and routed through the network. IP version 6 (IPv6) is a new version of the Internet Protocol, designed to gradually replace IP version 4 (IPv4), which, at the moment, is the de facto standard, especially within the Internet. IPv6 has been designed to have better addressing capability and integrated support for mobility. It retains the attractive features of IPv4 and reduces the unattractive ones. The most important change is that IPv6 increases the IP address size from 32 to 128 bits. Furthermore, the header format has been simplified and the concept of extension headers has been introduced. The adoption of IPv6 has been slowed by lack of device support and some remaining architectural problems, as well as by the introduction of Network Address Translation (NAT), which partially alleviates the problem of address exhaustion (Srisuresh & Egevang 2001).

IPsec is a group of security protocols and a standard for securing private communications over IP networks. It implements network layer encryption and authentication and is a compulsory part of IPv6 and optional in IPv4. (Kent & Atkinson 1998.) IPsec security protocols, such as Authentication Header (AH) and Encapsulating Security Payload (ESP), support authentication, data integrity and data confidentiality for packets travelling across the network.

Mobile IPv6 (MIPv6) is a protocol that allows nodes to remain reachable while moving around in the IPv6 Internet. Figure 3 illustrates a simplified MIPv6 connection.

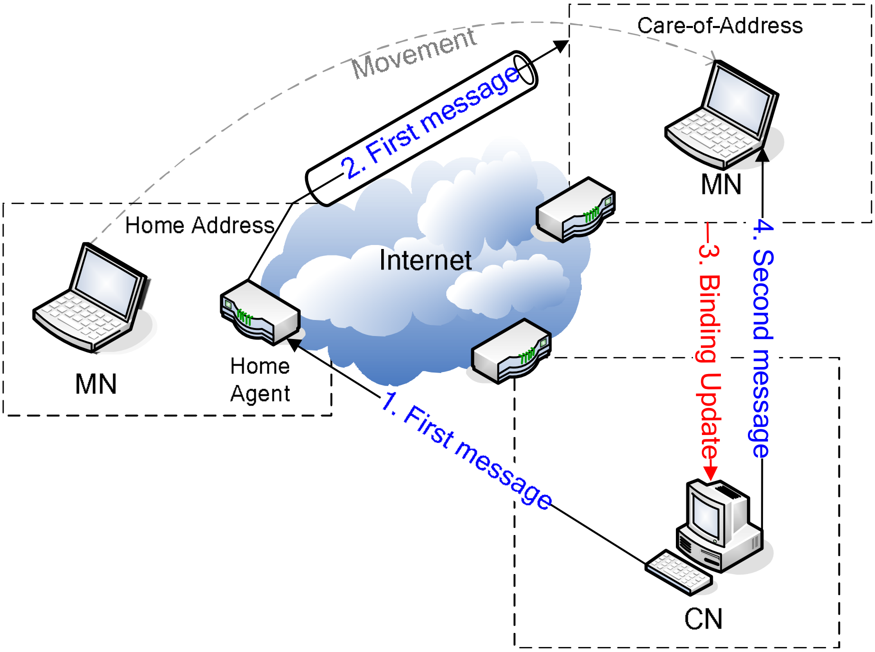


*Figure 3. Basic MIPv6 functionality.*

Each mobile node (MN) is always identified by its home address (HoA), regardless of its current point of attachment to the Internet. While situated away from its home, the MN is also associated with a care-of-address (CoA). The mobile node's Home Agent (HA) transparently routes IPv6 packets addressed to an MN's HoA to its CoA, after they have gone through a binding update (BU) procedure, where an association between the MN's HA and CoA is established and acknowledged by the HA. (Johnson et al. 2004.) Home Agent is a router in the MN's home network that keeps the location information for the MN when it moves to a foreign network. The communications between MN and HA are secured. The nodes the MN communicates with are called Correspondent Nodes (CN). A Correspondent Node may itself be either mobile or stationary.

When the MN has moved away from its home network, the CN will send the first message to the MN's HoA because it does not know the current location of the MN. The HA will receive all packets sent to the MN when it is away from home and then tunnel the packet to the MN's new location, the CoA. The MN itself sends packets directly to the CN. This scenario is known as triangle routing. As this is not very effective, MIPv6 also enables the MN and CN to communicate directly, without going through a home agent, by the use of the Mobile IPv6 Route Optimization. This is done using a procedure defined as Return Routability (RR) (Arkko et al. 2004; Johnson et al. 2004; Nikander et al. 2005). When the MN receives the tunnelled packet coming from the CN via a home agent, it can send a binding update message to the CN, giving its current CoA. The CN will register the new binding and send the next messages directly to the MN, thus avoiding triangle routing. The format of the most important MIPv6 protocol headers and messages for this study are further explained in Appendix B.

### 2.3.1 AODV and MIPv6 in MANETs

Figure 4 presents the TCP/IP protocol layered structure and shows where the AODV and MIPv6 protocols are situated in it.

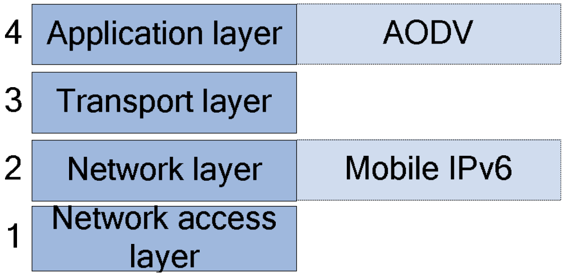


*Figure 4. TCP/IP protocol architecture and the position of AODV and MIPv6 in it.*

AODV can work together with mobile Internet protocols to create a hybrid wireless network that enables mobile nodes to connect to the Internet. In that case, AODV takes care of route discovery and maintenance of routes within the MANET and Mobile IP is used for the rest while it uses routing tables created by AODV. New protocols for optimising interconnection between the IP and the MANET are actively being researched (e.g. Lamont et al. 2003, Miao et al. 2004, Park et al. 2004, Theoleyre & Valois 2004, Wan et al. 2004). AODV can cooperate with IPv6 as well as IPv4. The only changes to the AODV protocol in the case of IPv6 are that the address fields are enlarged accordingly. There are certain difficulties in connecting MANETs to the Internet, but they are outside the scope of this study.

# 3. Network Security and Security Measurement

Information security refers to the protection of information in order to achieve and maintain the required level of protection. Information security can be seen as a quality attribute or a continual process. The security issues are complex, especially in the networks, and have a lot of different cross-relationships to consider. In addition to this study's point of view – which is intentional malicious attacks on the network – security can be compromised in many different ways, for example due to implementation errors as well as malfunctions or non-deliberate misuse of the system.

Measurement practices in the field of security are not as well established as in some other fields, even though measurement is a concrete way how the quality of the network and its security can be evaluated or monitored, and how to tell if the network security solutions are performing. It is desirable to define the security performance of the network based on something practical. Consequently, there is an obvious need for security metrics for MANETs as well as for other networks.

## 3.1 Network Security

Network security means the protection of networks and their services from unauthorised modification, destruction or disclosure. It involves the protection of network hardware, software and protocols, including information transmitted over networks.

A threat is usually defined as a circumstance, event or agent with potential to cause loss or harm. According to Pfleeger (1997, 394), there are four types of network threats: interruption, interception, modification and fabrication. They are illustrated in Figure 5 and explained in Table 2. All threats offend one or more information security dimensions. Most often, these dimensions are defined as confidentiality, integrity and availability. These information security dimensions are explained and the connections between them and network security threats are shown in Table 2.

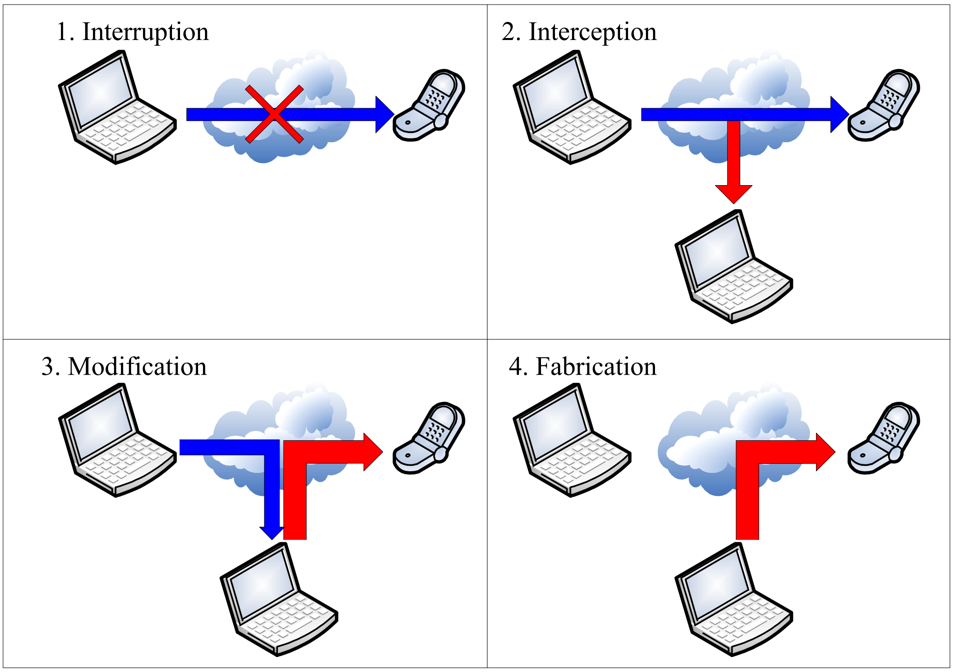


*Figure 5. Types of network security threats.*

Network security threats manifest themselves in a variety of attacks. In addition to the classifications of intentional and unintentional attacks, network attack types are divided into two main categories: active and passive. In active attacks the attacker penetrates the network and actively attempts to alter or destroy the data being transmitted. Passive attacks do not disrupt the operation of the network. Attacks threatening MANETs in particular were discussed in more detail in Chapter 2.

*Table 2. Information security dimensions and network security threats.*

| Information Security Dimension | Explanation | Network Security Threat |
|---|---|---|
| Confidentiality | Only authorised parties can access the information. | Interception =<br>Unauthorised access to data in transit. |

| | | |
|---|---|---|
| Integrity | Only authorised parties can modify or destroy the information, and only in authorised ways. Data must remain unchanged from the source to the destination. | Modification =<br>Unauthorised modification of the data in transit. |
| | | Fabrication =<br>Insertion of faked messages into the network. |
| Availability | Authorised parties always have access to timely, reliable information when needed. | Interruption =<br>Malicious destruction of a network element. |

## 3.2 Security Measurement

Measurement can be defined as the determination of the magnitude of a quantity or as a systematic process of data collection, repeated over time or at a single point in time. Measuring security is vital in order to be able to manage security based on the evidence of the achieved security performance.

The difference between measurement and metrics must be kept in mind. Measurements provide a one-time view of specific measurable parameters and are represented by numbers, weights or binary statements. On the other hand, metrics are produced by taking measurements over time and comparing two or more measurements with predefined baselines, thus providing a means for interpretation of the collected data (Sademies 2004).

Typically, information security metrics are seen as the basis for either evaluation or observation of system performance. Evaluation may include auditing, for example the Goal/Question/Metric (GQM) approach (van Solingen & Berghout 1999), or risk and vulnerability analysis, where the current state of risks and vulnerabilities and their anticipated consequences are assessed, or penetration testing. Observation of system performance usually means gathering and analysing various technical logs and inserting test cases simulating attacks or vulnerabilities. These approaches are still ambiguous and immature, and no commonly accepted information security metrics approaches yet exist.

According to Katzke (2001), security metrics in general currently lack precision and contain considerable uncertainty due to the immature discipline of the field.

The nature of the basic mechanisms of the MANETs causes extra vulnerabilities. For example, most of the intrusion detection techniques developed for fixed wired networks are not applicable to MANETs as there are no traffic concentration points where the intrusion detection systems could collect audit data for the entire network. (Chlamtac et al. 2003.) Obviously, distributed or node-level intrusion detection mechanisms are needed for MANETs.

### 3.2.1 Security Metrics Model

There are three important issues that should be taken into account when planning measurements and metrics. First, one should plan what to measure; second, how to measure it; and third, what to compare the results of the measurement with. In other words, as phrased by Savola and Holappa (2005), the following information should be gathered for each metric:

- metric objects: a collection of measurable objects to be measured
- metric methods: methods associated with the metrics
- metric measuring rod: a database associated with the metrics that consists of reference information classified according to the level of security. The measuring rod is based on an analysis of the security objectives.

The above-mentioned issues are also included in the security metrics model according to Katzke (2001). That model is illustrated in Figure 6.

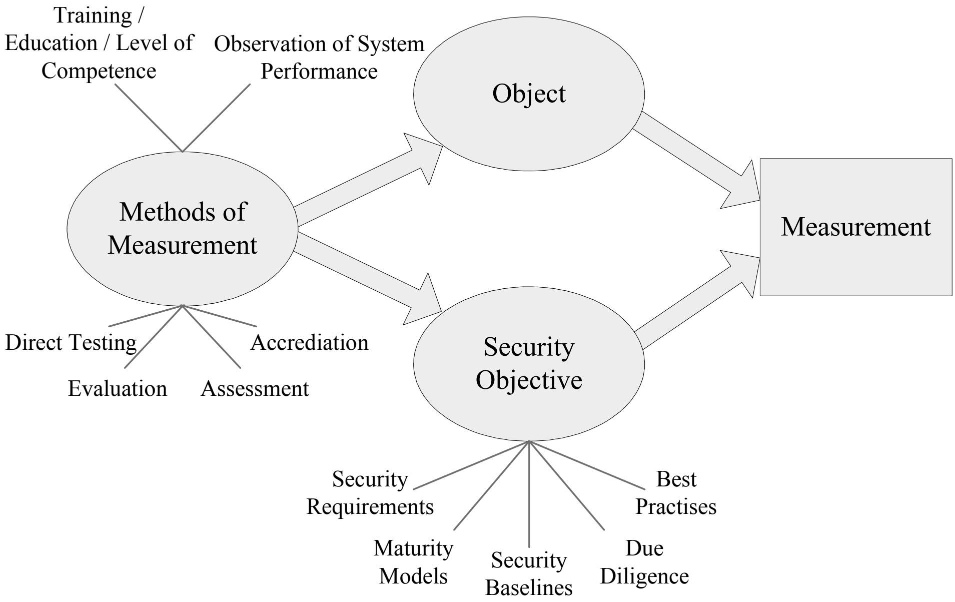


*Figure 6. Security metrics model (Katzke 2001).*

In general, the object that is measured does not necessarily have to be a product or system; it can be, for example, a security policy or the competence of the staff. In the model, six techniques have been specified as methods of measurement. A method can be based on human factors, such as the experience and training of the measurer. The performance of the measured system can also be observed. Different risk assessment techniques are widely used for the evaluation and assessment. Direct testing means functional tests, such as the penetration tests performed by “tiger teams”. The system’s accreditations are also considered measurement methods.

The methods for measuring should be chosen on the basis of the goal of the test, and this is why the security objectives are required. Measuring just for its own sake is no use, but when there is an objective that shows the goals for the object to meet, the results of the measurement can be useful. Five possible security objectives that can be bases for the measuring rods are mentioned in the model in Figure 6. Security requirements and baselines can be hierarchic and company-specific or universal standards and specifications, depending on the case at issue. The Common Criteria (Common Criteria 2004) is one well-known example of those baselines.

The majority of the few available security metrics approaches have been developed for evaluating the maturity of security engineering processes. The most developed and feasible of the maturity models in the information security field is perhaps the Systems Security Engineering Capability Maturity Model (SSE-CMM 2005). Due diligence refers to security management that is based on experience and level of competence. Best practices, like the BS7799/ISO17799 Code of practice for information security management (ISO/IEC 2005), are standards and collections of recommendations and requirements to be followed.

### 3.2.2 Classifications of Security Metrics

Security metrics can be divided into qualitative and quantitative, and classified into the next four categories (Henning 2002):

- technical metrics, for example risk and threat analyses and intrusion detection metrics
- operational metrics, which describe and manage the risks to operational environments
- organisational metrics, which describe and track the effectiveness of organisational programs and processes, for example audits
- integrated metrics, which refer to concepts of synthesis, cross-track issues and big-picture concerns.

The focus in this study is on the quantitative technical security metrics. According to Savola (2005), technical security metrics can be used for goal establishment, prediction before implementation or in an implemented system, comparison of the security level of technical objects, monitoring or scanning the security level of an object, and enabling analysis in fault injection testing for example. The methods of technical security measurement can fall into the categories shown in Table 3.

*Table 3. Categories of technical security measurement.*

| Category | Explanation |
|---|---|
| Certification | Certification is the classification of the system in classes based on the design characteristics and security mechanisms (Savola 2005). |
| Intrusion process measurement | Measurements of the intrusion process are statistical measurements of a system based on the effort it takes to make an intrusion (Savola 2005). The Intrusion Prevention System (IPS) and Intrusion detection system (IDS) are the most commonly used examples of the kind of measurement systems that are used for improving security. Intrusion prevention techniques, such as encryption and authentication, are usually the first line of defence in the network security. IPSs make access control decisions based on application content rather than IP address or ports as was done with traditional firewalls. IDSs are mostly deployed in the network environment. They are used to detect, identify and stop all types of malicious network traffic by analysing the information they gather and compare it with large databases of attack signatures. Essentially, IDSs look for a specific attack that has already been documented. |
| Network security monitoring | Network security monitoring is a comprehensive way of measuring security in a network. It extends IDS/IPS and includes collection, analysis and escalation of indications and warnings to detect and respond to intrusions (Bejtlich 2004). |
| Risk and vulnerability analysis | Risk analysis is an estimation of the probability of specific risks and vulnerabilities, and their consequences and costs. |
| Security measuring frameworks | Numerous security measuring frameworks have been constructed, but none of them are very extensive or universal. Some examples of different types of frameworks are authored by Alampalayam & Kumar (2003), Perkins et al. (2002), Raghavan & Dhyanesh (2002) and Xenakis & Merakos (2004). |
| Penetration testing | Tiger teams try to find security vulnerabilities in information systems by trying to simulate adversaries and obtain unauthorised access to information. |

Metrics can be used either proactively or reactively. In general, metrics are found most useful when they can be used proactively – predicting or trying to understand future situations (Savola 2005). MANET security can also be measured from the perspective of a single node (de-centralised) or from the perspective of a group of nodes (centralised). A hybrid of both perspectives (partly centralised) is also possible.

- Centralised measurement

  Measurement is carried out all around the network. The measured data is transferred via the network from one node to another and gathered at a single point that makes decisions based on it.

- De-centralised measurement

  Each node is responsible for its own measurements, and no measurement data is exchanged in the network. Each node makes its own decisions based on the data it has measured.

- Hybrid measurement

  Each node is responsible for its own measurements. The measured data is transferred via the network from a node to other nodes. Each node makes its own decisions based on the data gathered by itself or other nodes.

# 4. Attack Trees

Many approaches in security analysis are based on the idea of modelling the attacker's steps in attacking the system. Attack tree (Schneier 2000, 318–333) is an approach that provides a methodical way of describing threats against a system and thus helps in constructing an overall security model for a system.

Attack tree is represented by a structure of a tree growing upside down. A root node that represents the main goal of the attacker is at the top of the tree. In most cases several different approaches are possible to achieve this main goal. That goal is divided into increasingly detailed subgoals. Nodes below a particular node represent subtasks. The nodes can be either AND or OR nodes. Several subtasks beneath an AND node must be achieved in order to accomplish the node's goal. In other cases the node is called an OR node, where successfully performing any one (or more) of the subtasks will cause the goal to be accomplished. (Schneier 2000, 318–333.) The notation developed for the purpose of this study is introduced in Figure 7.

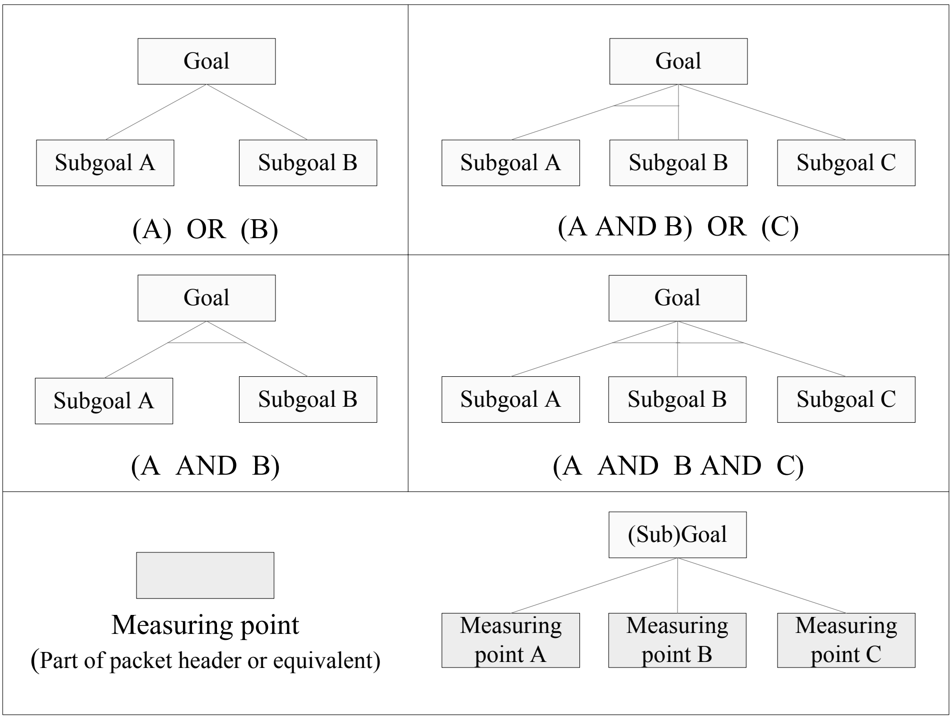


*Figure 7. The notation of attack trees used in this study.*

Networks have numerous vulnerable points. A single attack tree, or actually a single path in an attack tree, represents an opportunity for an attack against a network. In this study attack trees are made from three attack case examples against AODV and two attack case examples against MIPv6. The attack trees have been designed so that they are as general as possible yet go as deep as possible so that the actual bit flow of the data transmitted in the network is visible with the help of the attack trees. The measuring points can be defined when the lowest level of each attack has been reached. A measuring point means part of the protocol frame or packet header, the actual spot in the data where the attack may be noticeable.

In the case examples illustrated in the next sections nodes A and B are mobile devices that belong to a mobile ad hoc network. Node E is another mobile node but with malicious intentions, in other words node E is the attacker who tries to accomplish certain attacks either against node A or against both nodes A and B. However, one should bear in mind that these examples are only part of the whole picture. There are an enormous number of different attacks, and unintentional attack-like situations, malfunctions etcetera, which may look like attacks and harm the network.

## 4.1 Ad Hoc On-Demand Vector Protocol Case Examples

The next three subsections each illustrate case examples of attack trees regarding the AODV protocol. These examples have been chosen because they are very typical threats in MANETs, easy to accomplish and effective from the attacker's point of view. The found measuring points are further discussed in Chapter 5.

### 4.1.1 Black Hole Attack

MANETs' unique characteristics enable several ways to launch denial-of-service attacks. Black hole attack is one of the basic DoS attacks. It aims to isolate one node from its data traffic, as shown in Figure 8. Node E captures the messages directed to node A and does not transmit them any further. The attack tree in Figure 9 illustrates how the attacker first finds a way to get all node A's data and then either deletes it or uses it for his or her profit but does not transmit it to node A.

### 4.1.2 Man in the Middle Attack

Routing protocols, such as AODV, are primary targets for impersonation attacks. It is very difficult to determine the occurrence of impersonation attacks in networks where the node membership is not known (Perkins et al. 2003). To successfully complete a man-in-the-middle (MiM) attack the attacker has to convince both target nodes that it is the destination node. This can be done simply by sending false routing information. When the attacker knows that two nodes are communicating with each other he or she can send both nodes new, faked routing messages with a high sequence number claiming to be the other node with a new location. Then, according to the AODV specification, the nodes alter their routing tables and start communication with the attacker, who can start reading and possibly modifying data transmitted between these target nodes. This case is pictured in Figure 10, with the corresponding attack tree in Figure 11.

### 4.1.3 Resource Consumption Attack

It may be fairly easy to accomplish a resource consumption attack in a MANET. Some of the devices using the MANET can have very limited resources. For example, an elementary mobile phone cannot handle a very large data file, heavy encryption or large number of routing messages without either jamming the data communication channel or using all the processor or battery power. The resource consumption attack taking advantage of the limited resources of a node is illustrated in Figure 12, with the corresponding attack tree in Figure 13. In this example the attacker can waste the power resources of a node either by transmitting data to that node itself or by making other nodes do it by faking the routing information.

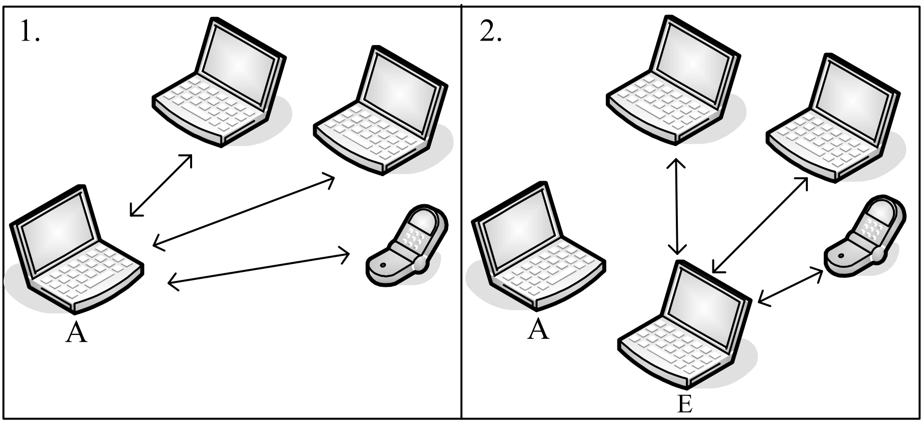


*Figure 8. A black hole attack in AODV.*

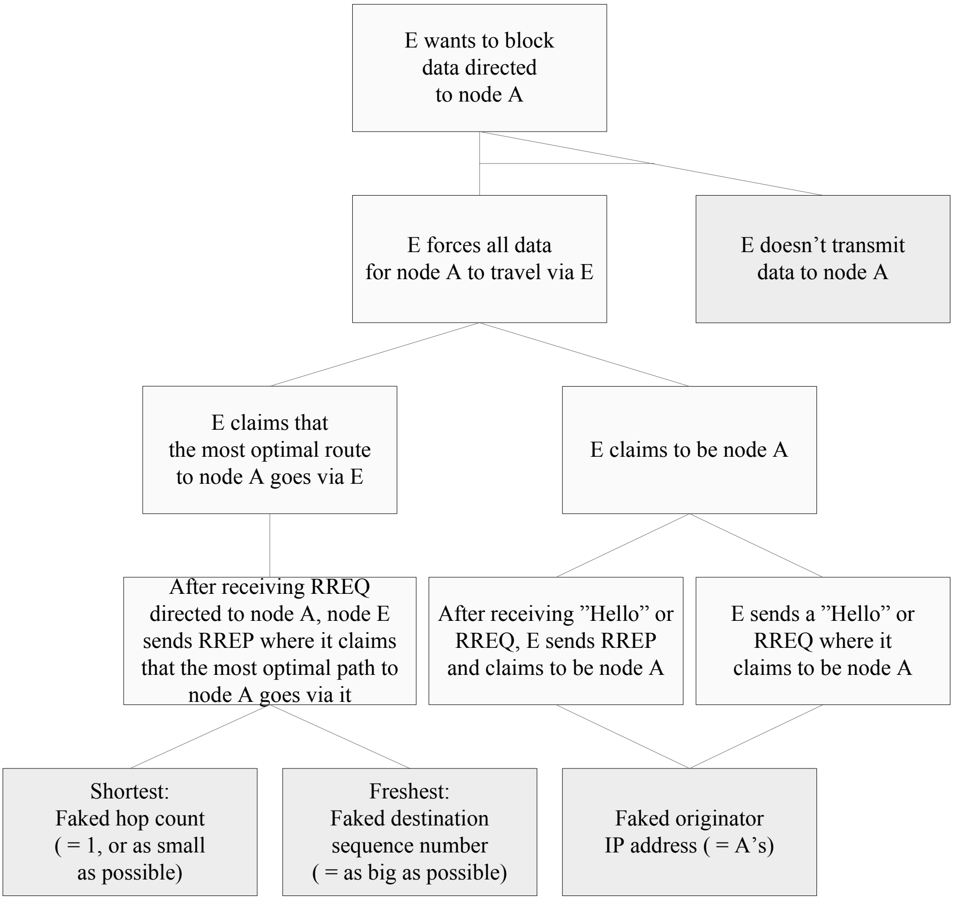

E wants to block data directed to node A
E forces all data for node A to travel via E
E doesn't transmit data to node A
E claims that the most optimal route to node A goes via E
E claims to be node A
After receiving RREQ directed to node A, node E sends RREP where it claims that the most optimal path to node A goes via it
After receiving "Hello" or RREQ, E sends RREP and claims to be node A
E sends a "Hello" or RREQ where it claims to be node A
Shortest: Faked hop count ( = 1, or as small as possible)
Freshest: Faked destination sequence number ( = as big as possible)
Faked originator IP address ( = A's)

*Figure 9. A case example attack tree of a black hole attack in AODV.*

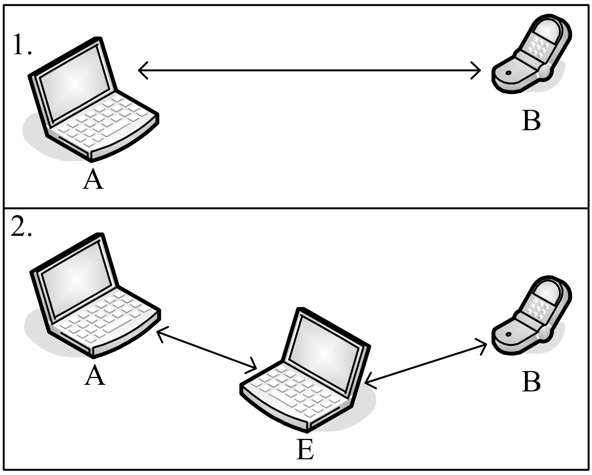


*Figure 10. A man-in-the-middle attack in AODV.*

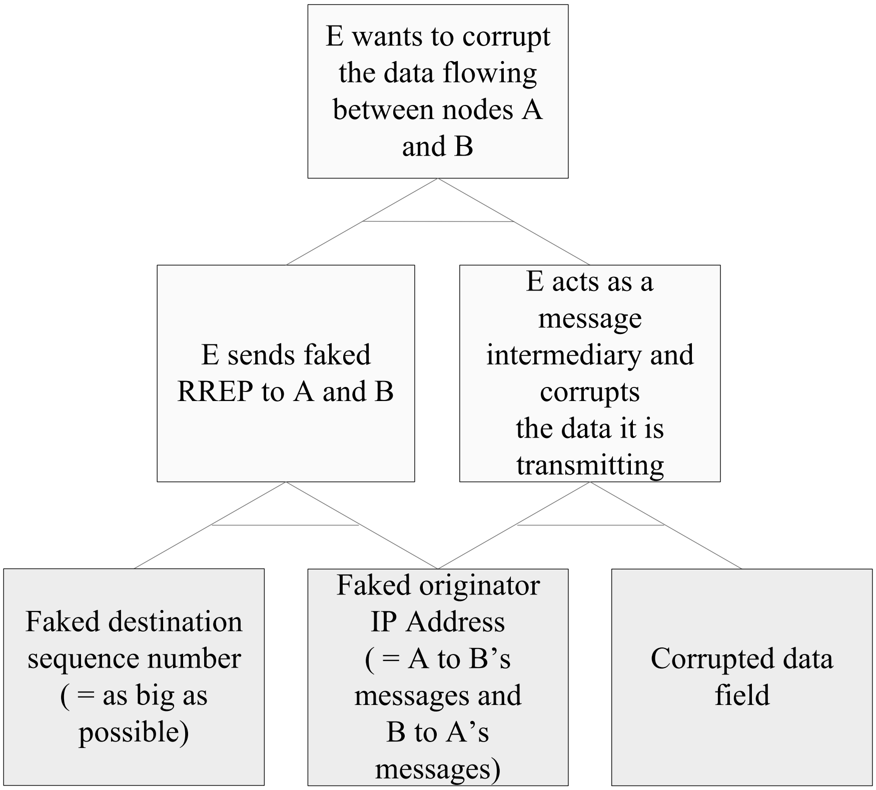

E wants to corrupt the data flowing between nodes A and B
E sends faked RREP to A and B
E acts as a message intermediary and corrupts the data it is transmitting
Faked destination sequence number ( = as big as possible)
Faked originator IP Address ( = A to B's messages and B to A's messages)
Corrupted data field

*Figure 11. A case example attack tree of a man-in-the-middle attack in AODV.*

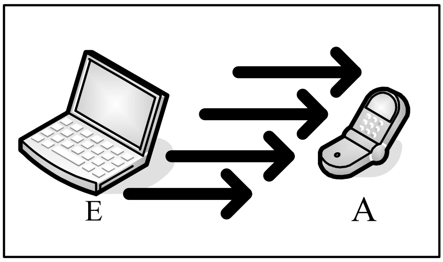


*Figure 12. A resource consumption attack in AODV.*

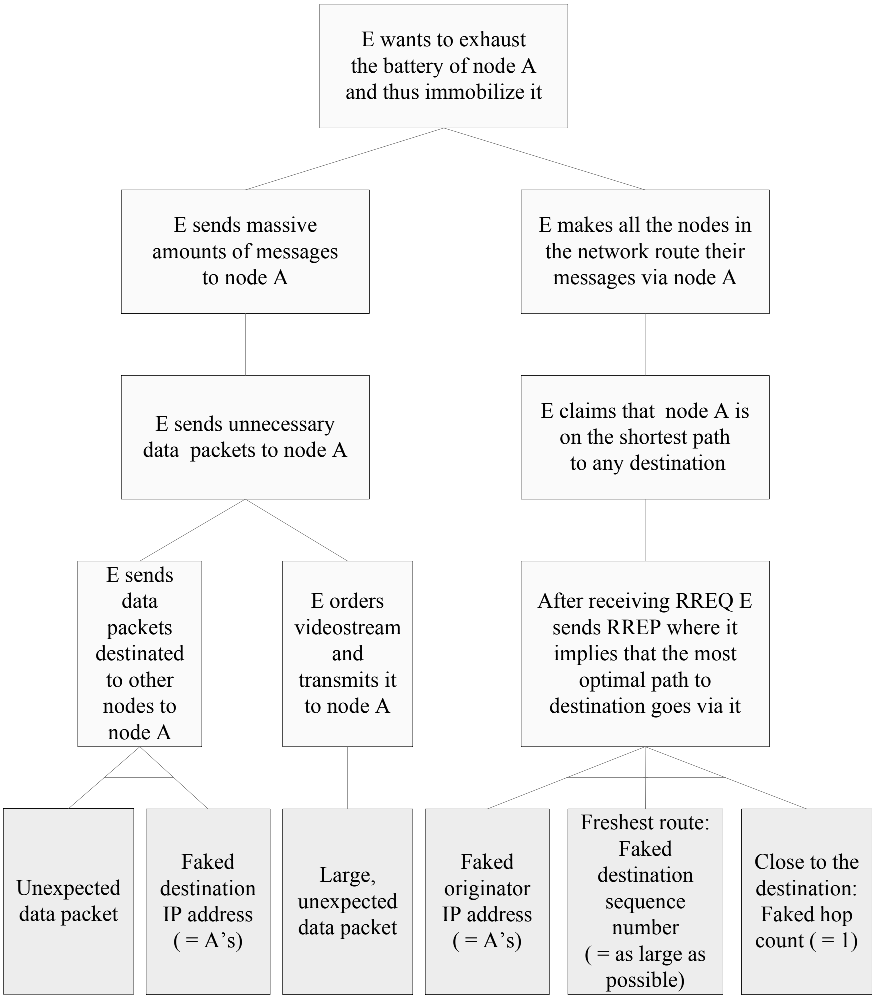

E wants to exhaust the battery of node A and thus immobilize it
E sends massive amounts of messages to node A
E makes all the nodes in the network route their messages via node A
E sends unnecessary data packets to node A
E claims that node A is on the shortest path to any destination
E sends data packets destinated to other nodes to node A
E orders videostream and transmits it to node A
After receiving RREQ E sends RREP where it implies that the most optimal path to destination goes via it
Unexpected data packet
Faked destination IP address ( = A's)
Large, unexpected data packet
Faked originator IP address ( = A's)
Freshest route: Faked destination sequence number ( = as large as possible)
Close to the destination: Faked hop count ( = 1)

*Figure 13. A case example attack tree of a resource consumption attack in AODV.*

## 4.2 Mobile Internet Protocol Version 6 Case Examples

The next two sections present attack trees of attacks regarding MIPv6. These examples have been chosen because they can be carried out in much the same way as the equivalent attacks regarding the AODV protocol, even though MIPv6 has many more security features than AODV. The man-in-the-middle attack, which is one of the examples with AODV, has intentionally been left out of the MIPv6 examples due to the high level of security protection in this protocol. For example, the Return Routability (Nikander et al. 2005) and ingress filtering (Baker & Savola 2004) security features can be used in MIPv6. So many assumptions and presuppositions about not using some of these available security features would have been required for trying to accomplish a full attack tree of a man-in-the-middle attack that it was found not to serve the interest of this study to have it as a case example. The found measuring points are further discussed in Chapter 5.

### 4.2.1 Black Hole Attack

Basically, the black hole attack situation in MIPv6 is the same as in AODV. Figure 14 illustrates the attack situation for MIPv6, with the corresponding attack tree in Figure 15. The main difference between these two attacks is that it is not possible to fake routing information in MIPv6 as easily as in AODV.

The easiest way for an attacker node to avoid the protection mechanisms included in MIPv6 is to just advertise itself as another node, with no care-of-addresses or such. This is not a foolproof method, as it is probably not possible to advertise yourself to every single node that might want to communicate with node A, but it may work within certain limits anyway. Consequently, node A probably receives some of its data and thus is not totally isolated, but at least some nuisance can be caused by this attack.

### 4.2.2 Resource Consumption Attack

Figure 16 illustrates an example of the resource consumption attack for MIPv6, with the corresponding attack tree in Figure 17. This attack is even easier with MIPv6 than with just AODV. Protocols with many security features can actually make the nodes more vulnerable to DoS attacks such as resource consumption. MIPv6 messaging requires a lot of resources from the node itself, and thus not that much interference is needed to exhaust them.

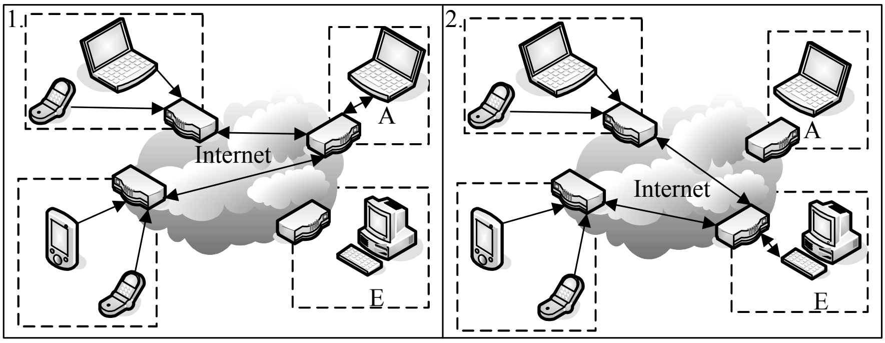


*Figure 14. A black hole attack in MIPv6.*

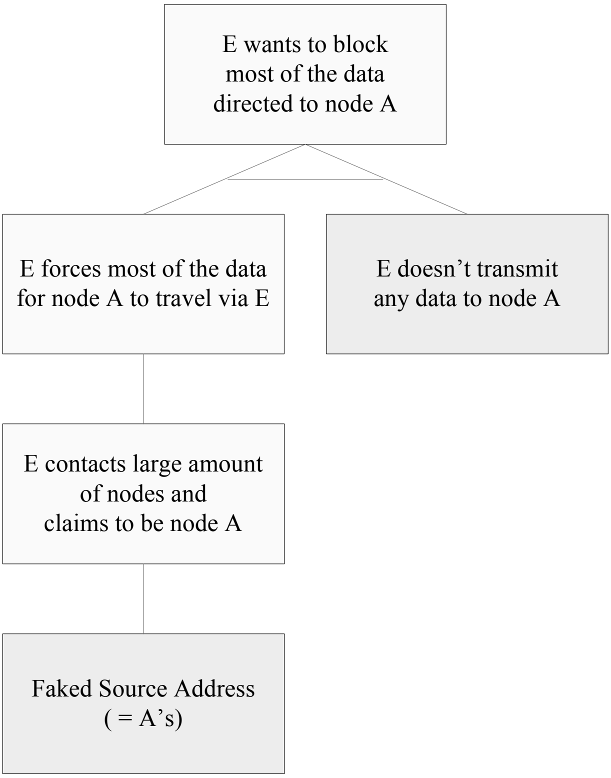

E wants to block most of the data directed to node A
E forces most of the data for node A to travel via E
E doesn't transmit any data to node A
E contacts large amount of nodes and claims to be node A
Faked Source Address ( = A's)

*Figure 15. A case example attack tree of a black hole attack in MIPv6.*

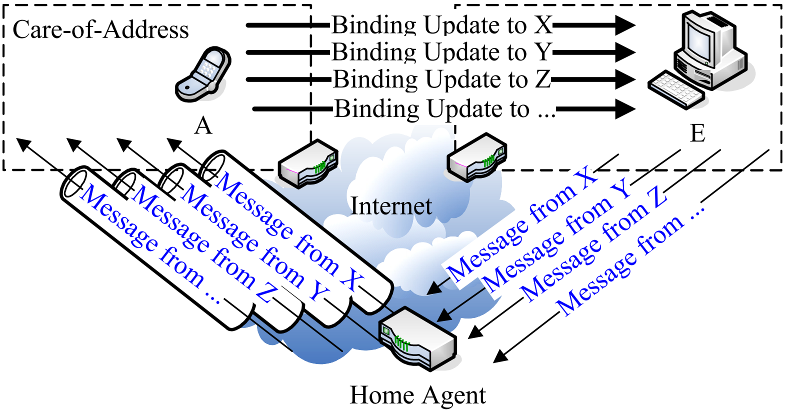


*Figure 16. An example of a resource consumption attack in MIPv6.*

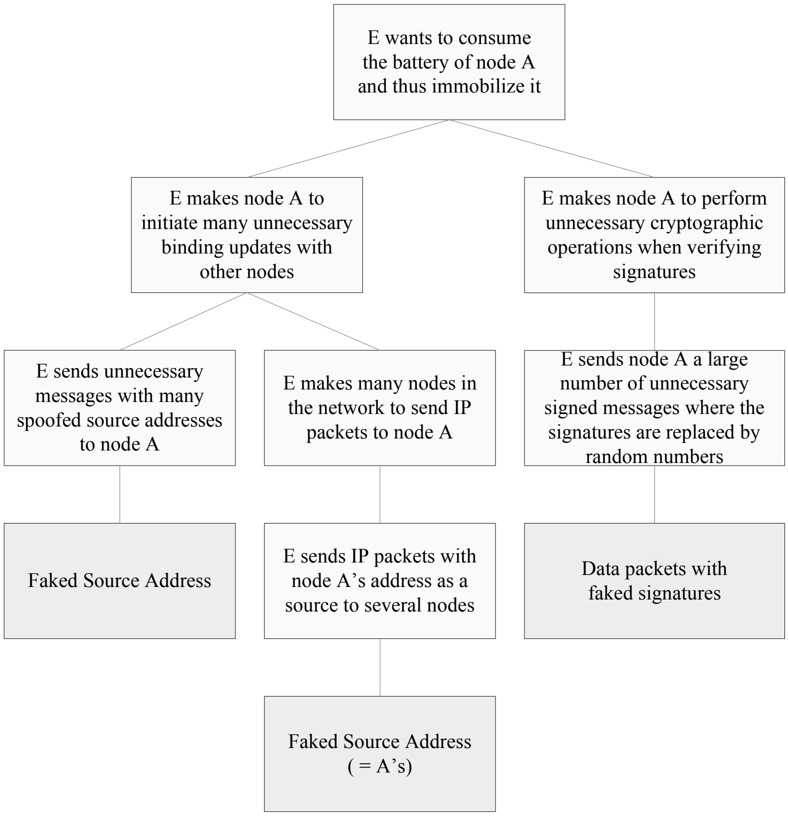

E wants to consume the battery of node A and thus immobilize it
E makes node A to initiate many unnecessary binding updates with other nodes
E makes node A to perform unnecessary cryptographic operations when verifying signatures
E sends unnecessary messages with many spoofed source addresses to node A
E makes many nodes in the network to send IP packets to node A
E sends node A a large number of unnecessary signed messages where the signatures are replaced by random numbers
Faked Source Address
E sends IP packets with node A's address as a source to several nodes
Data packets with faked signatures
Faked Source Address ( = A's)

*Figure 17. A case example attack tree of a resource consumption attack in MIPv6.*

# 5. Analysis of Attack Tree Case Examples

Based on Schneier's (2000) description of attack trees and their usage possibilities, it was assumed that the attack tree approach would be a very applicable way of finding points in the network where security measurements can be taken. In this chapter the measuring points found from the case examples in Chapter 4 are gathered up and some analysis of these examples is made. Further analysis of the general results of this study is given in Chapter 6.

Three different types of measuring points are found based on the attack tree case examples:

1. Part of the message header, for example part of an RREP message.
2. Actual data that was transferred between the nodes, for example size or content information about the transferred data.
3. Behaviour of a node where it does not follow the basic rules of MANETs, for example a node does not transmit messages it is supposed to transmit.

These different types of found measuring points are pictured in Figure 18. However, the metadata and node behaviour types are not analysed in this study because the focus here is on the network protocols and their functions.

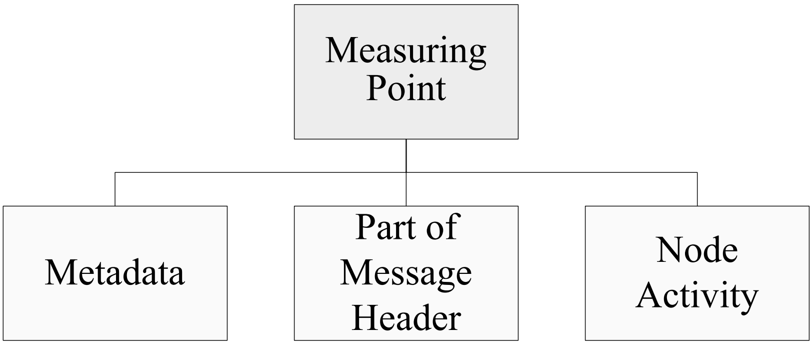


*Figure 18. The different types of measuring points found in the case examples.*

## 5.1 Ad Hoc On-Demand Vector Protocol Cases

The AODV case examples are discussed in this chapter. The headers of the appropriate AODV routing messages are shown in Figure 19, where the measuring points according to the attack tree examples are highlighted.

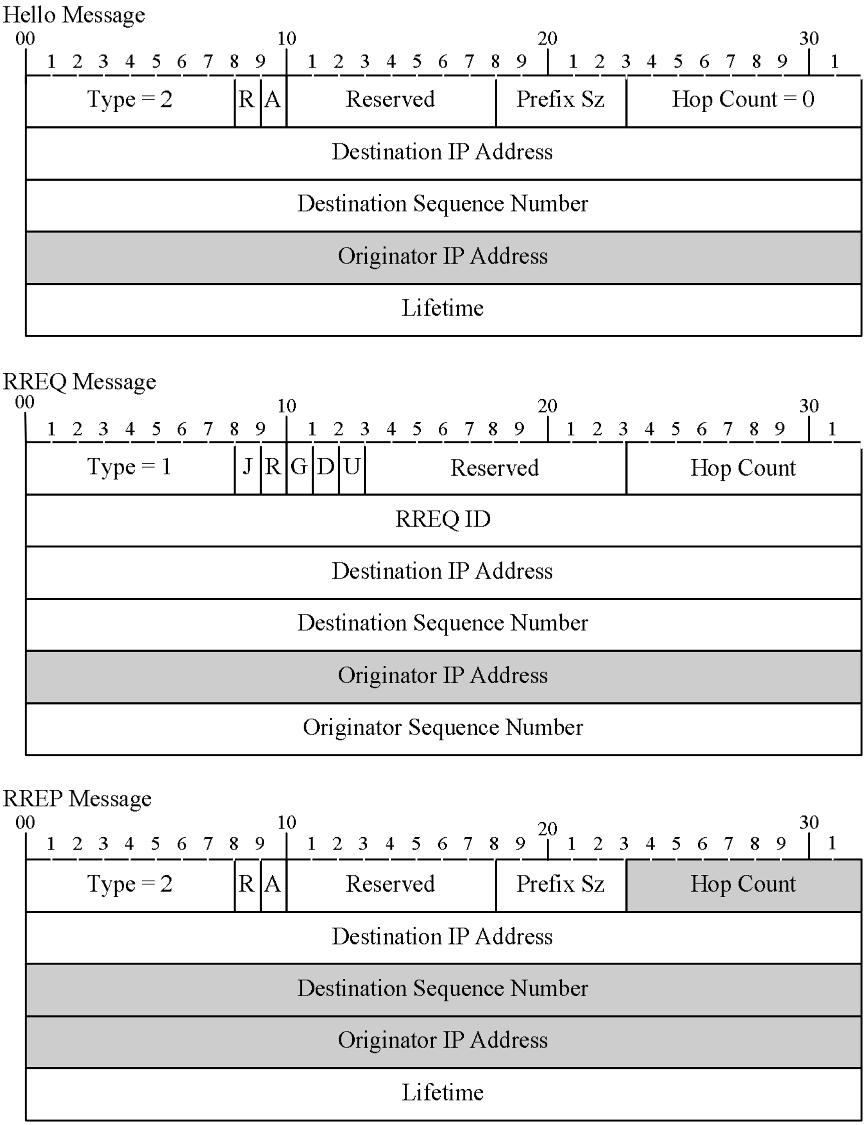


*Figure 19. Summary of the message header measuring points according to the AODV case examples.*

The first case is a black hole attack (Figure 9). There are four separate measuring points in this example. Three of them (faked originator IP address, faked hop count and faked destination sequence number) are of the message header types and one (no data transmission) is of the node activity type. The second case is a man-in-the-middle attack (Figure 11). Three measuring points can be found in that attack tree, of which two (faked originator IP address and faked destination sequence number) are of the message header type and one (corrupted data) is of the metadata type. The third AODV attack tree case is a resource consumption attack (Figure 13). Four of the found measuring points (faked originator IP address, faked destination IP address, faked hop count and faked destination sequence number) are message header types and again one (large, unexpected data) is of the metadata type. These results are also pictured in Table 4.

*Table 4. Summary of the measuring points in the AODV attack tree examples.*

| Figure number | Attack | Measuring point | Measuring point type |
|---|---|---|---|
| 9 | Black hole | Faked originator IP address<br>Faked hop count<br>Faked destination sequence number | Message header |
| | | No data transmission | Node activity |
| 11 | Man-in-the-middle | Faked originator IP address<br>Faked destination sequence number | Message header |
| | | Corrupted data | Metadata |
| 13 | Resource consumption | Faked originator IP address<br>Faked destination IP address<br>Faked hop count<br>Faked destination sequence number | Message header |
| | | Large, unexpected data | Metadata |

Based on these examples, three routing messages (“Hello”, RREQ and RREP) should be investigated in more detail. The RREP message is the most vulnerable part; almost all the case attacks could be found by measuring the RREP message. In the RREP message, both the originator IP address field and the destination sequence number field, if faked, could give signals of any of these three attacks. Those fields appear in all three attack trees. The destination IP address field only appears in one of the examples, in the resource consumption attack tree, and even there it is part of the metadata type of message and not within the focus of this study. The hop count field appears in two out of three attack trees. These results are summarised in Table 5.

*Table 5. The relationship between the found measuring points and the attacks in AODV.*

| Routing message type | Originator IP address field | Destination sequence number field | Hop count field |
|---|---|---|---|
| "Hello" | Black hole | – | – |
| RREQ | Black hole | – | – |
| RREP | Black hole,<br>Man-in-the-middle,<br>Resource consumption | Black hole,<br>Man-in-the-middle,<br>Resource consumption | Black hole,<br>Resource consumption |

## 5.2 Mobile Internet Protocol Version 6 Cases

The header of the IPv6 message as well as the Mobility header with Binding Update message are shown in Figure 20.

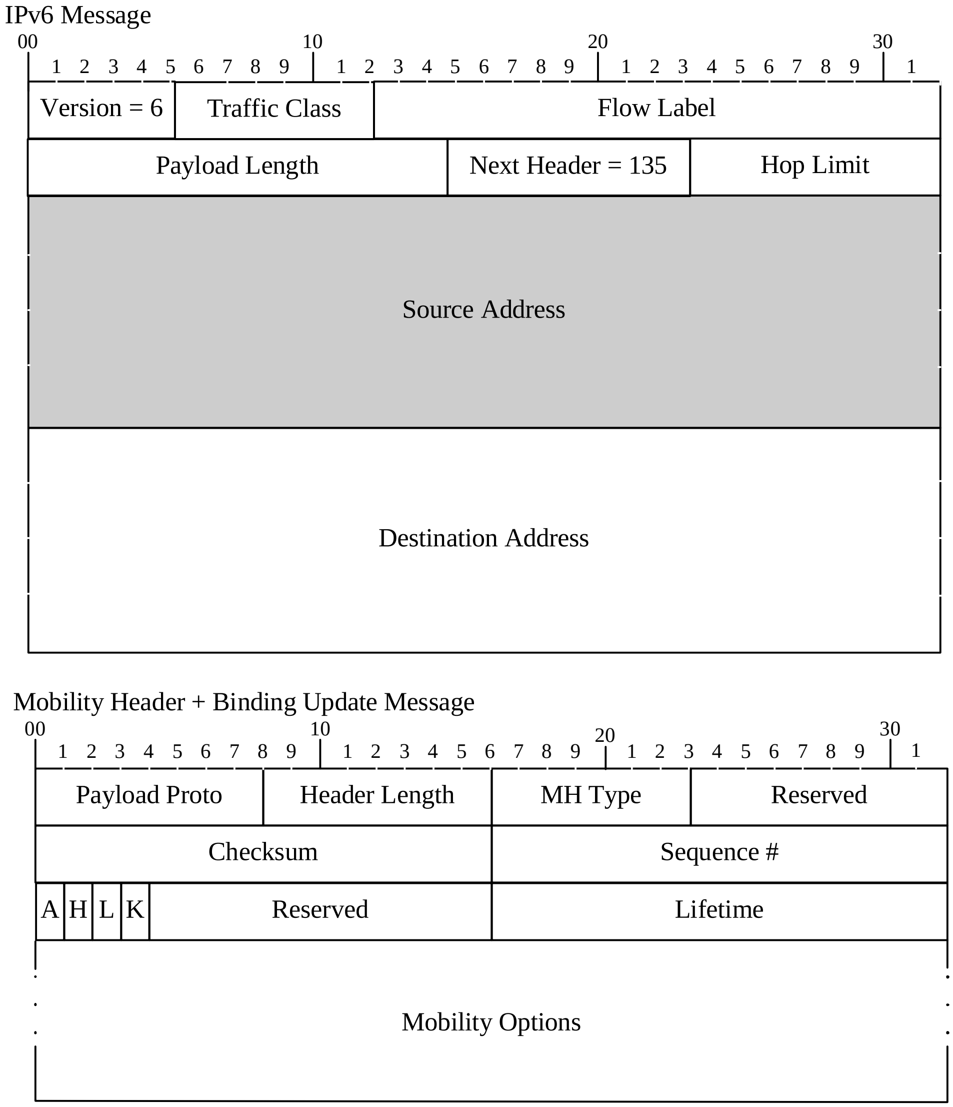


*Figure 20. Message header measuring point according to the MIPv6 case examples.*

The first MIPv6 attack tree case example is a black hole attack (Figure 14). There are two measuring points in this example. One of them (faked source address) is of the message header type and the other one (no data transmission) is of the node activity type. In fact, this example is exactly the same with IPv6 as with MIPv6; there is no specific mobility issue involved in this case. The second case is the resource consumption attack (Figure 15). This attack tree is more specific to Mobile IPv6, as the binding update procedure is specified in the MIPv6 protocol. Two measuring points be found in this example, of which one (faked source address) is of the message header type and the other (data with faked signatures) is of the metadata type. These results are also pictured in Table 6.

*Table 6. Summary of the measuring points in MIPv6 attack tree examples.*

| Figure number | Attack | Measuring point | Measuring point type |
|---|---|---|---|
| 14 | Black hole | Faked source address | Message header |
| | | No data transmission | Node activity |
| 15 | Resource consumption | Faked source address | Message header |
| | | Data with faked signature | Metadata |

The same message field, Source Address, is found to be a measuring point in both of the MIPv6 attack trees. Based on these two MIPv6 examples, the message chains, which aim to start either the Binding Update procedure or some other communication, should be looked into in more detail to detect impersonations.

## 5.3 Summary of the Case Example Results

The attack tree examples in Chapter 4 cover all the types of network security threats discussed in Chapter 3. The black hole attack is an example of an interruption situation, where a node in the network does not receive the messages that it should. The man-in-the-middle attack has elements of both interception and modification threats. Depending on the case, the man-in-the-middle attack can intercept the messages and not transmit them forward, or transmit them with modified data, which is the case in our example. The resource consumption attack includes a fabrication threat, where extra data is supplied to the network to exhaust the resources of either one node or the whole network.

The results of the case examples indicated vulnerabilities in the two protocols under consideration. The difference between these protocols was significant due to their different design perspectives on security issues. Finding attacks that could be accomplished while avoiding such security features as required authentication is very easy with AODV and very demanding with MIPv6, and this is also visible in the results. In addition, the results are directly proportional to the complexity of the attack tree examples. The more branches there are in a tree, the more measuring points are found in it. It must be emphasised that the examples in this study are by no means exhaustive; the attack trees could be spread wider to include dozens of branches if the goal were to construct a comprehensive attack tree with all the possible ways of a certain attack.

This study gives initial results on which parts of the headers would be worthwhile to measure in order to define the security level of a network. In the case of the AODV protocol, both the destination sequence number and the hop count fields can be used as measuring points. The first, the destination sequence number, is probably more significant because the attacker would most likely be able to take more advantage of a faked destination sequence number than of a faked hop count. A high destination sequence number signifies a very fresh route, and the freshest routes are always updated to the routing tables in AODV. If the attacker's goal is to get a certain route to the routing tables of the network nodes, he is most likely to forge that field.

One common feature with the two protocols is that in all these attacks, and, respectively, in all the attack trees, the sender's address was found to be vulnerable to forgery. As obvious as it is, this is a relevant finding, especially when it is found to appear with both AODV and MIPv6. The basic difference between the AODV and the MIPv6 examples is that the AODV attack examples mainly consist of forged fields whereas the MIPv6 examples mostly consist of the apparently normal message transmissions but with malicious intentions; there are less forged fields in the MIPv6 examples. This difference is due to the strong security features of MIPv6, which ensure that unnoticeable faking of the message fields is a lot more difficult with MIPv6 than with AODV.

# 6. Discussion

The attack tree approach is one attempt at finding practical methods for measuring the security performance of a network. As no measurement can be done before the object of the measurement has been defined, the goal in this study was to clarify which fields of specific protocols in a specific network environment could be considered valid objects of security measurement.

In this study we have shown that some measuring points in the data transferred in the network can be found using attack trees. Although this is a tiny step in the process of finding the ultimate solution for network security measuring, it is far from insignificant. The significance of the work comes from breaking the ice, making an attempt to find practical ways of measuring security in a MANET environment.

Next, we report our observations on the various areas in this study and analyse the different aspects that came our way during the research.

## 6.1 On Security Measurement

Information security measurement is still a quite abstract concept. Some fragments of it have been researched but the whole concept needs to be properly defined, clarified and standardised. Network monitoring in general is at quite a high level already – for example, many quality attributes of the network can be measured. State-of-the-art network monitoring systems can also be used for measuring security, but there are still many open issues and challenges. In order to allocate the resources correctly, we first need to know what we are looking for, and where and how we can find it. Only then, when we know what data in the network is worth measuring, can we start using the existing network monitoring systems for security issues.

In this study, focusing on mobile ad hoc networks, some questions of importance arose. It is worth giving a lot of consideration to how cost-effective it is to use part of the devices' very limited resources for measurement. Even though measuring is important in order to be able to state facts about a network's security, good arguments for the value of such measurement would be needed to reason why a node should value measurement practices more than some other actions. The situations in which no measurement is needed should also be recognised.

Furthermore, interpretation of the measurement results should be available. To successfully measure the security of a MANET, a comprehensive database with good, up-to-date reference and threshold information for each of the metrics is necessary. The location of that database is no easy matter in this field. There are strong reasons why a node should have its own database, but there are also reasons for a centralised database. The same reasoning also concerns measuring. It is possible that every node is responsible for its actions based on the measurement results, but there can also be centralised actions.

In the case of network protocol measuring, the amount of data taken under the spotlight should be considered. Single data packets may sometimes be worth measuring, but every now and then a more effective way might be the measurement of packet sequences. The chain of events can often reveal more attacks than just one event. The actions taken after an attack is suspected should also be clearly defined. It is probable that in some cases the communication with a probable attacker must be cut off at once, while in some other cases some, maybe limited, communication can be continued. Various ways of actions should be specified according to various cases. More research on the whole wide area of information security measuring is needed.

## 6.2 On Attack Trees

An analysis based on attack trees has many advantages. It is easy to adopt and use with no need for special tools. It is suitable for various contexts and makes it possible to determine any level of abstraction, depending on the need, as well as keep track of the chain of actions. Attack trees can also be used for numerical assessments as they offer the possibility to assign values to the nodes of the tree, such as cost, impact or severity of attack. Furthermore, they enable both technical and non-technical analysis, and a wide variety of attacks can be found by using them. The attack tree approach is an excellent, illustrative basic method of finding measurable objects because it forces one to analyse different possibilities and threats in a systematic way, and this analysis is well documented too. And it can be used proactively, which is always good when dealing with information security phenomena.

The main drawback to the attack tree approach is probably its poor scalability. Evidently it is possible to construct a fully comprehensive attack tree with all the possibilities and contributing factors, but a true expert, or group of experts, as well as lot of time and effort, are needed to develop it manually. As a consequence, the attack tree inevitably becomes very complex and extensive with numerous branches and levels, ultimately losing its illustrative nature. Either the attack tree includes all imaginable subnodes and is no longer wholly manageable, or it is very clear and easy to use but only comprises part of the picture, just like the case examples in this study.

In the context of network protocols, where the situations and events are diverse and change a lot depending on each case, it would probably be useless to construct fully comprehensive attack trees for each situation manually. Though it is possible to re-use the attack trees or parts of them, we think that it most likely is not cost effective to spend the vast resources needed for the initial construction of attack trees for network traffic evaluation. It must also be borne in mind that there may be situations in the network that look exactly like intentional attacks but are either non-deliberate attack-like incidents or maybe even just the normal functionality of the network. These cases would also be falsely registered as attacks by the attack tree analyses, just as they are with almost all kinds of network monitoring tools.

All things considered, there are many positive and promising sides to the attack trees. In general, attack trees assist in analysing the security of systems and finding the weakest links by documenting almost all potential and probable attacks. Attack tree analysis well quantifies the security vulnerabilities of a system based on the goals of the attacker. We can think of many environments in which attack trees would fit extremely well. However, as long as there are no automatic tools for creating attack trees, they are not that feasible in the mobile ad hoc network environment due to the complexity and variability of the field.

We stress a couple of things we find extremely important concerning the attack trees. First, if a complete attack tree is aspired to, it is essential to construct it with a multitude of experts to cover all the aspects, options and factors of the area in question, both technical and non-technical. Automation would also be helpful in attack tree construction. Second, it must be remembered that this is just one aspect of information security. Attack trees cannot detect all of the security incidents, threats and vulnerabilities of the network because not all of them are attacks. There are accidents, bad programming or software design and other flaws and malfunctions that can compromise the security of the network just as much as the attacks.

## 6.3 On Mobile Ad Hoc Networks and Protocols

MANETs are very multipurpose and useful in certain situations. They have many advantages compared with traditional networks and it can be predicted that their usage will grow a good deal in the future. That is why the security issues regarding MANETs should really be solved quickly, at least at a reasonable level. Of course, if a MANET is only built up for a short period of time, and between two nodes that know each other, there are fair reasons to assume that only an acceptable number of information security threats exist in that network. But already now, and more and more increasingly in the future, there are long-term MANETs with hundreds of nodes, where security threats are an everyday reality.

The fact that the chosen attack cases in this study concern MANETs had great effect on this study. One of the main and most challenging features in MANETs is that there is no central administration. This makes the detection of attacks, as well as measuring the network activities, much more demanding than it would be in a more traditional kind of network. When all the nodes are expected to act as a router and be equal in the network, it is hard to figure out which node to trust fully. A reasonable conclusion is that a node can only fully trust itself, and, in some cases, such as multi-user systems, maybe not even itself. Nevertheless, co-operation with some of the nodes would most likely be very worthwhile, if one only could decide which nodes to trust. One conclusion about MANETs is quite obvious: in the future, in order to get some security features to work fully, we will probably have to make trade-off decisions concerning the equality of the nodes and decide that some nodes in the network are more equal than others.

Of the network protocols used in MANET, the AODV and MIPv6 protocols are examined in this study. They act on different levels in the network and have different tasks to accomplish. They are very suitable for this study as they are both relatively new protocols and their usage and significance will grow in the years to come. The fact that AODV does not have any security features while MIPv6 has many of them causes some trouble during the attack tree construction. It is very difficult for a non-hacker-minded person to find functional, clear and illustrative attacks against MIPv6 without setting too many constraints or assumptions about the circumstances.

There are plenty of examples of resource consumption attacks in MANETs. It cannot be stressed too much that resource problems are the core security issue in MANETs. The devices in MANETs are of multiple resource levels and the low capacity nodes should be able to survive, hence the protocols and ways of action in MANETs should be as resource-friendly as possible. The fact that all the nodes act as routers consumes a lot of their energy. Some of the nodes might drop out if security features like authentication and encryption are added. Measurement consumes resources as well so the nodes must have good resource management where the priorities of various functions are defined. This sets challenges; the advantages of security measuring practices should be obvious to the nodes in order to avoid neglect of these practices.

A few observations on protocol messages must also be expressed, although they have already been explained to some extent in the analysis in Chapter 5. It must be remembered that the examples constructed in this study are just a few out of thousands and thousands of possibles, so it is difficult to claim that the results are general enough. However, according to the examples in this study, some messages and fields of protocol headers appear to be more prone to be targeted by an attacker than some others. Regardless of the attack, the most evident spot worth measuring in AODV is the destination sequence number, as well as the originator address. In MIPv6, the source address field is the number one measuring point, but the binding update procedure is vulnerable to several malicious actions as well.

## 6.4 On Attacks

In contrast to the examples in this study, attacks can be implemented against the whole network instead of just one node. Furthermore, there might be more than one malicious node in the network, or an attacker could combine different types of attacks consecutively to make the attacks more damaging. If the attacks are distributed so that they come from several sources, the threat is much more severe, finding the  attackers is more difficult, the attacks can be done faster and the damage done can be more fatal than it would be in the case of a single attacker. For example, two co-operating attackers can send large packets of data between each other and congest the whole network, even when acting perfectly by the specifications of the network. The “virtually correct actions but malicious intentions” attacks against the MIPv6 protocol are especially practical for an attacker. If the attacker knows how the network operates, it is easier to carry out these virtually correct but malicious actions than to try to find a way around the various protections.

# 7. Conclusions

This study aimed at the identification of measuring points in a mobile ad hoc network by applying the attack tree method. This is a necessary initial phase when planning security measurements. The approach presented in this study is novel: topics that have not yet been investigated, even independently – attack trees, security measurement and mobile ad hoc networks – were studied in a consolidated way.

Based on the results of study, attack trees can well be utilized in general situations concerning security measurement, but they do not work very well in complex networked environments, such as mobile ad hoc networks, if applied manually. The main drawback to the attack tree approach is its poor scalability; in mobile ad hoc networks attack trees are not readily feasible due to their inherent complexity and variability. It would probably be pointless to construct comprehensive attack trees for each situation manually. Automation is needed for full exploitation of this method.

There are major differences between the security features of the two protocols used, and the results of applying attack tree analysis differ depending on the protocol. The AODV protocol, with less security features, clearly has more vulnerable message fields than MIPv6. It must be noted that there are some common vulnerabilities as well; the address fields of a sender node are vulnerable in both of the protocols.

Devices typically have very limited resources in a mobile ad hoc network environment. This sets limits on the protocols that can be successfully used in that environment and on the security solutions and measurements that can be applied. In order to fully utilise the measurement results we would probably have to make trade-off decisions concerning the equality of the nodes and decide that some nodes in the network are more equal than some others. However, this does not follow the classical ad hoc principle in mobile ad hoc networks.

Future research and practical experimentation in this area is still needed in order to deploy attack trees in security monitoring, and for MANETs specifically. The attack tree approach should be used in various network environments to find its optimal use. It would also be worth constructing some heuristics concerning the node activity and the metadata of the data transferred within the network. Moreover, an analytical basis for heuristics for measuring the security of MANETs should be developed in order to develop the attack tree analysis mechanisms further. Some effort should also be put into finding a way of separating the situations that appear to be intentional attacks but are not.

To conclude, it is still difficult to state that a certain network is secure enough. The attack tree approach can be a useful method for exploring vulnerabilities in a systematic way and incorporating measuring points. However, it was also observed that they are not very suitable for assessing attacks at the level of network protocols if applied manually. This is due to the complexity and diversity of the information networks, which causes the attack trees to inevitably grow uncontrollably large. The study also shows that a greater number of vulnerable message fields could clearly be found in the network protocol with less security features (AODV) than the other (MIPv6), but both protocols share the vulnerability of the sender node’s address field.

# References

Alampalayam, S.P. & Kumar, A. 2003. Security Model for Routing Attacks in Mobile Ad Hoc Networks, IEEE 58th Vehicular Technology Conference. VTC 2003-Fall, p. 2122–2126.

Arkko, J., Devarapalli, V. & Dupont, F. 2004. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. IETF Request for Comments: 3776. [Web-document.] Available: http://www.ietf.org/rfc/rfc3776.txt. [Referenced 15.8.2005.]

Baker, F. & Savola, P. 2004. IETF Request for Comments: 3704, BCP: 84. Ingress Filtering for Multihomed Networks. [Web-document.] Available: http://www.ietf. org/rfc/rfc3704.txt. [Referenced 15.8.2005.]

Bejtlich, R. 2004. The Tao of Network Security Monitoring: Beyond Intrusion Detection. Boston: Addison-Wesley.

Chlamtac, I., Conti, M. & Liu, J.J.-N. 2003. Mobile Ad Hoc Networking: Imperatives and Challenges. Ad Hoc Networks. Vol. 1, no. 1, p. 13–64.

Common Criteria. 2004. Common Criteria for Information Technology Security Evaluation, Version 2.2. [Web-document.] Available at: http://www.commoncriteriaportal.org/public/expert/index.php?menu=2/. [Referenced 16.3.2005.]

Deering, S. & Hinden, R. 1998. Internet Protocol, Version 6 (IPv6) Specification. IETF Request for Comments: 2460. [Web-document.] Available: http://www.ietf.org/rfc/rfc2460.txt. [Referenced 12.5.2005.]

Henning, R. 2002. Proceedings of the Workshop on Information Security System Scoring and Ranking. 2001, Williamsburg. [Web-document.] Available: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf. [Referenced 10.2.2005.]

ISO/IEC. 2005. International Organization for Standardization. Information Technology – Security Techniques – Code of Practice for Information Security Management. ISO/IEC 17799:2005(E). Geneva: ISO Copyright Office.

Johnson, D., Perkins, C. & Arkko, J. 2004. IETF Request for Comments: 3775. Mobility Support in IPv6. [Web-document.] Available: http://www.ietf.org/rfc/rfc3775.txt. [Referenced 10.2.2005.]

Katzke, S. 2001. Security Metrics. [Web-document.] Available: http://www.cs.msstate. edu/~ia/IA_PAPERS/Katzke.pdf. [Referenced 23.1.2005.]

Kent, S. & Atkinson, R. 1998. IETF Request for Comments: 2401. Security Architecture for the Internet Protocol. [Web-document.] Available: http://www.ietf.org/rfc/rfc 2401.txt. [Referenced 16.8.2005.]

Lamont, L., Wang, M., Villasenor, L., Randhawa, T. & Hardy, S. 2003. Integrating WLANs & MANETs to the IPv6 based Internet. ICC '03. IEEE International Conference on Communications. Vol. 2, p. 1090–1095.

Miao, F., Xiong, Y., & Yang, S. 2004. A Mobile Ad Hoc Internet Interconnection Technology based on Mobile IP. Mini-Micro Systems. Vol. 25, no. 1, p. 24–29.

Nikander, P., Arkko, J., Aura, T., Montenegro, G. & Nordmark, E. 2005. Mobile IP Version 6 Route Optimization Security Design Background. Internet-Draft. [Web-document.] Available: http://www.ietf.org/internet-drafts/draft-ietf-mip6-ro-sec-03.txt. [Referenced 16.8.2005.]

Park, I., Kim, Y. & Lee, S. 2004. IPv6 Address Allocation in Hybrid Mobile Ad-Hoc Networks. In: Proceedings of Second IEEE Workshop on Software Technologies for the Future Embedded and Ubiquitous Systems, p. 58–62.

Perkins, C.E., Malinen, J.T., Wakikawa, R., Nilsson, A. & Tuominen, A.I. 2002. Internet Connectivity for Mobile Ad Hoc Networks. Wireless Communications and Mobile Computing. Vol. 2, no. 5, p. 465–482.

Perkins, C., Belding-Royer, E. & Das, S. 2003. Ad Hoc On-Demand Distance Vector (AODV) Routing. IETF Request for Comments: 3561. [Web-document.] Available: http://www.ietf.org/rfc/rfc3561.txt. [Referenced 14.2.2005.]

Pfleeger, C.P. 1997. Security in Computing. 2nd edition. Upper Saddle River: Prentice Hall PTR.

Raghavan, S.V. & Dhyanesh, N. 2002. Formal Description of Perfect Security. Redefining Internet in the Context of Pervasive Computing. Proceedings of 15th International Conference on Computer Communication, p. 1113–1120.

Sademies, A. 2004. Process Approach to Information Security Metrics in Finnish Industry and State Institutions. VTT Publications 544. Espoo: VTT. Available: http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf.

Savola, R. 2005. Estimation of the Security Level in a Mobile and Ubiquitous Environment based on Semantic Web. In: Proceedings of the 7th International Conference on Enterprise Information Systems (ICEIS 2005). Vol. 4, p. 256–262.

Savola, R. & Holappa, J. 2005. Self-Measurement of the Information Security Level in a Monitoring System Based on Mobile Ad Hoc Networks. In: Proceedings of the 2005 IEEE Int. Workshop on Homeland Security, Contraband Detection and Personal Safety, p. 42–49.

Schneier, B. 2000. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons.

van Solingen, R. & Berghout, E. 1999. The Goal/Question/Metric method: a practical guide for quality improvement of software development. London: McGraw-Hill.

Srisuresh, P. & Egevang, K. 2001. IETF Request for Comments: 3022. Traditional IP Network Address Translator. [Web-document.] Available: http://www.ietf.org/rfc/rfc3022.txt. [Referenced 16.8.2005.]

SSE-CMM. 2005. Systems Security Engineering Capability Maturity Model. The International Systems Security Engineering Association. [Web-document.] Available: http://www.sse-cmm.org/. [Referenced 25.1.2005.]

Tanenbaum, A.S. 1996. Computer Networks. 3rd edition. Upper Saddle River: Prentice Hall PTR.

Theoleyre, F. & Valois, F. 2004. A Virtual Structure for Hybrid Networks. IEEE Wireless Communications and Networking Conference WCNC. Vol. 2, p. 1040–1045.

Wan, X., Yao, Y. & Wang, H. 2004. New Clustering Algorithm for Interconnection of MANET and Internet. Journal of Systems Engineering and Electronics. Vol. 15, no. 1, p. 83–89.

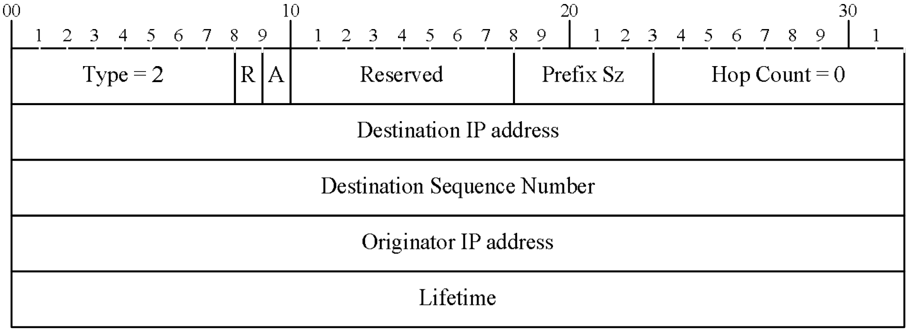
Xenakis, C. & Merakos, L. 2004. Security in Third Generation Mobile Networks. Computer Communications. Vol. 27, no. 7, p. 638–650.

# Appendix A: AODV Message Formats

Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs) are the message types defined by AODV. The “Hello” message type is a slightly altered type of Route Reply. These message types are received via UDP, and normal IP header processing applies. (Perkins et al. 2003.)

The formats of the messages are illustrated first, and the fields are explained in the following tables according to the AODV protocol specification by Perkins et al. (2003).

### “Hello” Message Format

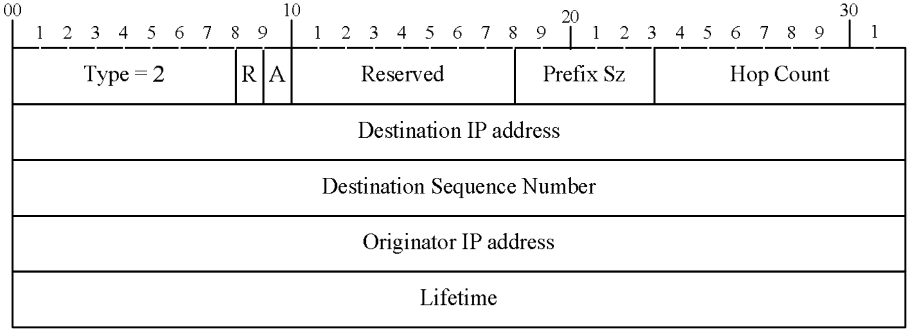


| Field | Explanation |
|---|---|
| Type | 2 for RREP (“Hello”) |
| R | Repair flag; used for multicast. |
| A | Acknowledgement required |
| Reserved | Sent as 0; ignored on reception. |
| Prefix Size | If non-zero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination. |
| Hop Count | 0 |
| Destination IP Address | The originator node’s IP address. |
| Destination Sequence Number | The originator node’s latest sequence number. |
| Originator IP Address | The IP address of the node that originated the RREQ for |

| | |
|---|---|
| | which the route is supplied. |
| Lifetime | ALLOWED_HELLO_LOSS * HELLO_INTERVAL, as defined by the node. The default values are ALLOWED_HELLO_LOSS = 2 and HELLO_INTERVAL = 1,000 Milliseconds. |

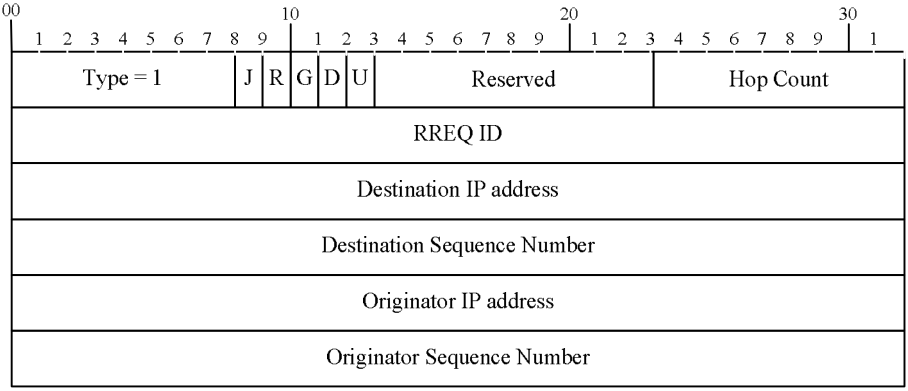
The “Hello” message is a special case of RREP. It is separated from the RREP by the IP header, where the TTL field is 1 in the case of a “Hello” message.

## Route Reply (RREP) Message Format



| Field | Explanation |
|---|---|
| Type | 2 for RREP |
| R | Repair flag; used for multicast. |
| A | Acknowledgement required |
| Reserved | Sent as 0; ignored on reception. |
| Prefix Size | If non-zero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination. |
| Hop Count | The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP. |
| Destination IP Address | The IP address of the destination for which a route is supplied. |
| Destination Sequence Number | The destination sequence number associated with the route. It helps in avoiding routing loops and identifying the freshness of the route. It is created by the destination to be included along with any route information it sends to requesting nodes. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number. A larger sequence number denotes a fresher route. If several paths have the same sequence number, the shortest one is chosen. (Perkins et al. 2003.) |
| Originator IP Address | The IP address of the node that originated the RREQ for which the route is supplied. |
| Lifetime | The time in milliseconds for which nodes receiving the RREP consider the route to be valid. |

## Route Request (RREQ) Message Format



| Field | Explanation |
|---|---|
| Type | 1 for RREQ |
| J | Join flag; reserved for multicast. |
| R | Repair flag; reserved for multicast. |
| G | Gratuitous RREP flag; indicates whether a gratuitous RREP should be unicast to the node specified in the Destination IP Address field |
| D | Destination only flag; indicates that only the destination may respond to this RREQ |
| U | Unknown sequence number; indicates that the destination sequence number is unknown |
| Reserved | Sent as 0; ignored on reception. |
| Hop Count | The number of hops from the Originator IP Address to the node handling the request. |
| RREQ ID | A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address. |
| Destination IP Address | The IP address of the destination for which a route is desired. |
| Destination Sequence Number | The latest sequence number received in the past by the originator for any route towards the destination. |
| Originator IP Address | The IP address of the node that originated the Route Request. |
| Originator Sequence Number | The current sequence number to be used in the route entry pointing towards the originator of the route request. |

# Appendix B: MIPv6 Message Formats

The format of the IP package, as well as the mobility header with Binding Update message, are illustrated in the following pages, and the corresponding fields are explained in the following tables according to the IPv6 protocol specification by Deering and Hinden (1998) and the MIPv6 protocol specification by Johnson et al. (2004).

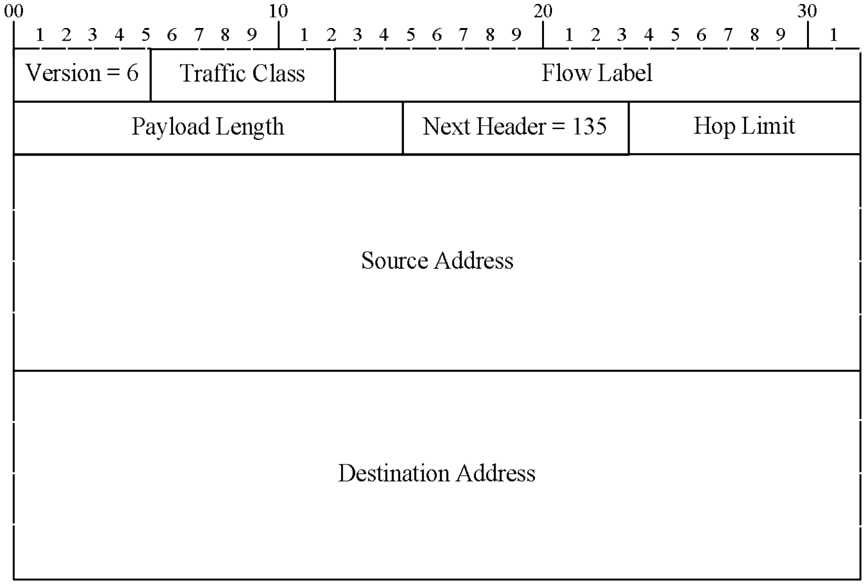
**IPv6 Extension Headers**

In IPv6 the optional Internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. The IPv6 packet may carry zero, one, or more extension headers, each identified by the Next Header field of the preceding header. The extension headers must be processed strictly in the order they appear in the packet. When more than one extension header is used in the same packet, it is recommended that those headers appear in the following order:

- IPv6 header
- Hop-by-Hop Options header
- Destination Options header
- Routing header
- Fragment header
- Authentication header
- Encapsulating Security Payload header
- Destination Options header
- Upper-layer header.

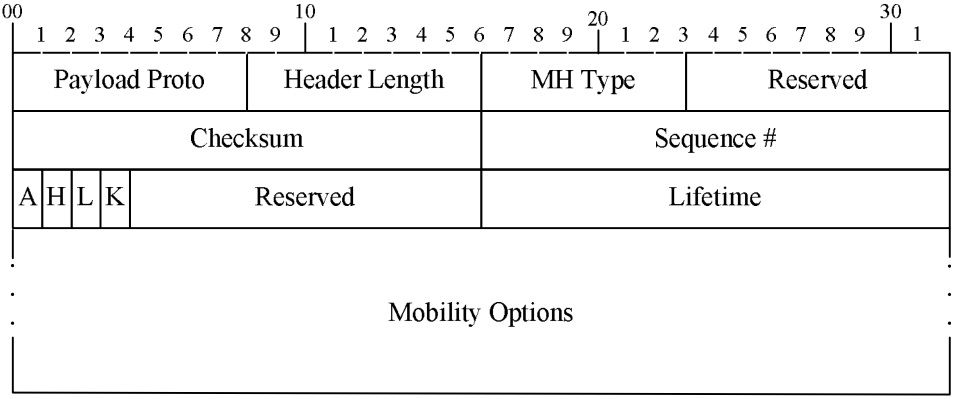
The fields of each extension headers are specified in detail in the IPv6 specification (Deering & Hinden 1998).

## IPv6 Message Format



| Field | Explanation |
|---|---|
| Version | 4-bit Internet Protocol version number = 6. |
| Traffic Class | 8-bit traffic class field. The default value must be zero for all 8 bits. |
| Flow Label | 20-bit flow label. Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet. |
| Payload Length | 16-bit unsigned integer. Length of the IPv6 payload – i.e., the rest of the packet following this IPv6 header – in octets. |
| Next Header | 8-bit selector. Identifies the type of header immediately following the IPv6 header. The value 59 in the Next Header field of an IPv6 header or any extension header indicates that there is nothing following that header. The value 135 in the Next Header field indicates that the mobility header is following next. |
| Hop Limit | 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if the Hop Limit is decremented to zero. |
| Source Address | 128-bit address of the originator of the packet. |
| Destination Address | 128-bit address of the intended recipient of the packet (possibly not the ultimate recipient if a Routing header is present). |

## Mobility Header with Binding Update Message



| Field | Explanation |
|---|---|
| Payload Proto | 8-bit selector. Identifies the type of header immediately following the Mobility Header. This field is intended to be used by a future extension. Implementations conforming to this specification SHOULD set the payload protocol type to IPPROTO_NONE (59 decimal). |
| Header Length | 8-bit unsigned integer, representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets. The length of the Mobility Header MUST be a multiple of 8 octets. |
| MH Type | 8-bit selector. Identifies the particular mobility message in question. An unrecognized MH Type field causes an error indication to be sent. |
| Reserved | 8-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver. |
| Checksum | 16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is calculated from the octet string consisting of a “pseudo-header” followed by the entire Mobility Header starting with the Payload Proto field. The checksum is the 16-bit one’s complement of the one’s complement sum of this string. For computing the checksum, the checksum field is set to zero. |
| Sequence # | A 16-bit unsigned integer used by the receiving node to sequence Binding Updates and by the sending node to match a returned Binding Acknowledgement with this Binding Update. |
| Acknowledge (A) | The Acknowledge (A) bit is set by the sending mobile node to request a Binding Acknowledgement (Section 6.1.8) be returned upon receipt of the Binding Update. |
| Home Registration | The Home Registration (H) bit is set by the sending mobile node to request that the receiving node should act as this node’s home agent. |

| | |
|---|---|
| (H) | The destination of the packet carrying this message MUST be that of a router sharing the same subnet prefix as the home address of the mobile node in the binding. |
| Link-Local Address Compatibility (L) | The Link-Local Address Compatibility (L) bit is set when the home address reported by the mobile node has the same interface identifier as the mobile node's link-local address. |
| Key Management Mobility Capability (K) | If this bit is cleared, the protocol used for establishing the IPsec security associations between the mobile node and the home agent does not survive movements. It may then have to be rerun. (Note that the IPsec security associations themselves are expected to survive movements.) If a manual IPsec configuration is used, the bit MUST be cleared. This bit is only valid in Binding Updates sent to the home agent, and MUST be cleared in other Binding Updates. Correspondent nodes MUST ignore this bit. |
| Reserved | These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver. |
| Lifetime | 16-bit unsigned integer. The number of time units remaining before the binding MUST be considered expired. A value of zero indicates that the Binding Cache entry for the mobile node MUST be deleted. (In this case the specified care-of address MUST also be set equal to the home address.) One time unit is 4 seconds. |
| Mobility Options | Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options it does not understand. |

Published by

Series title, number and report code of publication

VTT Publications 580
VTT–PUBS–580

Author(s)
Karppinen, Kaarina

Title

# Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment

Abstract

Practical evidence of the actual security performance of network systems is needed in order to be able to manage them in an adequate way.

This study investigates whether the attack tree approach can be used for identification of the appropriate data to be measured in a mobile ad hoc network environment, and whether divergent results of attack tree analysis are obtained with different types of network protocols. The study focuses on the data transmitted in the network in connection with attacks against the Ad hoc On-demand Distance Vector protocol (AODV) and Mobile Internet Protocol version 6 (MIPv6). The network type and the protocols used in this study were chosen because of their novelty and their potential importance in future communication scenarios.

Based on the results of the study, the attack tree approach is a helpful systematic method for exploring vulnerabilities. However, it is not suitable for a very detailed analysis of the attacks in the area of network protocols when applied manually. This is due to the complexity and diversity of information networks, which causes attack trees to inevitably grow uncontrollably large. Furthermore, this study shows that the results obtained by applying attack tree analyses differ depending on the protocol.

Keywords
security measurement, attack trees, mobile ad hoc networks, network protocols, network security, mobile internet protocol, data transfer, vulnerability, evaluation

Activity unit
VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FI–90571 OULU, Finland

| | | | |
|---|---|---|---|
| ISBN<br>951–38–6671–8 (soft back ed.)<br>951–38–6672–6 (URL:http://www.vtt.fi/inf/pdf/ ) | | | Project number<br>E5SU00573 |
| Date<br>October 2005 | Language<br>English, Finnish abstr. | Pages<br>57 p. + app. 8 p. | Price<br>B |
| Name of project<br>TRUST, MMAUTO | | Commissioned by | |
| Series title and ISSN<br>VTT Publications<br>1235–0621 (soft back ed.)<br>1455–0849 (URL: http://www.vtt.fi/inf/pdf/) | | Sold by<br>VTT Information Service<br>P.O.Box 2000, FI–02044 VTT, Finland<br>Phone internat. +358 20 722 4404<br>Fax +358 20 722 4374 | |

Julkaisija

Julkaisun sarja, numero ja raporttikoodi

VTT Publications 580
VTT–PUBS–580

Tekijä(t)
Karppinen, Kaarina

Nimeke

# Hyökkäyspuihin perustuva tietoturvan mittaaminen liikkuvassa spontaanissa (Ad Hoc) verkkoympäristössä

Tiivistelmä

Konkreettisia todisteita tietoverkkojen todellisesta turvallisuudesta tarvitaan, jotta tietoverkkoja voidaan hallita oikealla tavalla.

Tämä tutkimus pyrkii selvittämään, voidaanko hyökkäyspuumallia käyttää hyväksi soveliaan mitattavan tiedon määrittämiseen liikkuvassa spontaanissa (ad hoc) verkkoympäristössä ja saadaanko erityyppisillä verkkoprotokollilla toisistaan poikkeavia tuloksia hyökkäyspuutulosten analysoinnissa. Tutkimus keskittyy Ad hoc On-demand Distance Vector- (AODV) ja Mobile Internet Protocol version 6 (MIPv6) -protokolliin kohdistuvien hyökkäysten aikana verkossa kulkevaan dataan. Tutkimuksessa käytettävä verkkotyyppi ja verkkoprotokollat valittiin niiden uutuusarvon perusteella ja siksi, että niiden oletetaan olevan tärkeitä tulevaisuuden tietoliikenteessä.

Tutkimustulosten perusteella hyökkäyspuumalli on hyödyllinen menetelmä haavoittuvuuksien tutkimiseen. Manuaalisesti tehtynä se ei kuitenkaan sellaisenaan sovellu hyvin erittäin yksityiskohtaiseen verkkoprotokolla-alueen hyökkäysten analysointiin, koska tietoverkot ovat niin monimuotoisia ja kompleksisia, että hyökkäyspuut kasvavat väistämättä hallitsemattoman suuriksi. Tutkimuksessa havaittiin myös, että hyökkäyspuuanalyysin tulokset olivat erilaisia tutkimuksen kohteena olevasta verkkoprotokollasta riippuen.

Avainsanat
security measurement, attack trees, mobile ad hoc networks, network protocols, network security, mobile internet protocol, data transfer, vulnerability, evaluation

Toimintayksikkö
VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU

| | |
|---|---|
| ISBN<br>951–38–6671–8 (nid.)<br>951–38–6672–6 (URL: http://www.vtt.fi/inf/pdf/) | Projektinumero<br>E5SU00573 |

| Julkaisuaika | Kieli | Sivuja | Hinta |
|---|---|---|---|
| Lokakuu 2005 | Englanti, suom. tiiv. | 57 s. + liitt. 8 s. | B |

| Projektin nimi | Toimeksiantaja(t) |
|---|---|
| TRUST, MMAUTO | |

| Avainnimeke ja ISSN | Myynti: |
|---|---|
| VTT Publications<br>1235–0621 (nid.)<br>1455–0849 (URL: http://www.vtt.fi/inf/pdf/) | VTT Tietopalvelu<br>PL 2000, 02044 VTT<br>Puh. 020 722 4404<br>Faksi 020 722 4374 |

VTT PUBLICATIONS 580 Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment Kaarina Karppinen

This study investigates network security measurement based on attack trees. The attack tree method provides a systematic way of describing threats against a network and can be useful for exploring vulnerabilities as well as for incorporating measuring points, which are needed in security measurements.

The focus is on the data transmitted in a mobile ad hoc network in connection with attacks against the Ad hoc On-demand Distance Vector protocol (AODV) and Mobile Internet Protocol version 6 (MIPv6). The aim is the identification of measuring points, which is a necessary initial phase when planning security measurements. The attack trees of the case attacks are constructed and analysed, and the analysis results of these two divergent network protocols are compared.

Practical evidence of the actual security performance of network systems is needed in order to be able to manage them in an adequate way. This study presents a novel approach to attack trees, security measurement and mobile ad hoc networks - topics that have not yet been thoroughly investigated even independently - and studies them in a consolidated way.

| Tätä julkaisua myy | Denna publikation säljs av | This publication is available from |
|---|---|---|
| VTT TIETOPALVELU<br>PL 2000<br>02044 VTT<br>Puh. 020 722 4404<br>Faksi 020 722 4374 | VTT INFORMATIONSTJÄNST<br>PB 2000<br>02044 VTT<br>Tel. 020 722 4404<br>Fax 020 722 4374 | VTT INFORMATION SERVICE<br>P.O.Box 2000<br>FI–02044 VTT, Finland<br>Phone internat. +358 20 722 4404<br>Fax +358 20 722 4374 |

ISBN 951-38-6671-8 (soft back ed.)
ISSN 1235-0621 (soft back ed.)

ISBN 951-38-6672-6 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455-0849 (URL: http://www.vtt.fi/inf/pdf/)