(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2005 050 584 B4** 2009.04.30

(12) **Patentschrift**

(21) Aktenzeichen: **10 2005 050 584.8**
(22) Anmeldetag: **21.10.2005**
(43) Offenlegungstag: **16.05.2007**
(45) Veröffentlichungstag der Patenterteilung: **30.04.2009**

(51) Int Cl.[8]: ***H04L 12/56*** (2006.01)
H04L 12/26 (2006.01)

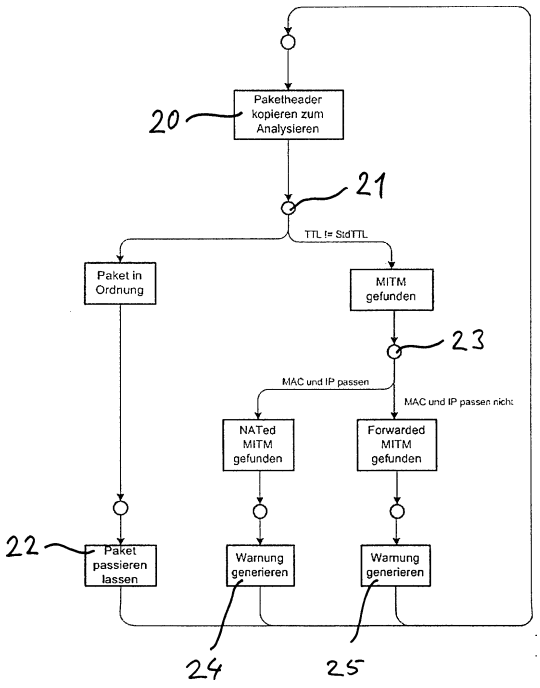
(73) Patentinhaber:
Will, Lucas, 14482 Potsdam, DE

(72) Erfinder:
Roschke, Sebastian, 14482 Potsdam, DE; Will, Lucas, 14482 Potsdam, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US2002/00 73 338 A1
US 2005/0 22 020 A1
US 2003/1 45 232 A1
US 2002/0 31 134 A1
GODBER,Austin, DASGUPTA,Partha: Countering Rogues in Wireless Networks. IEEE, Proceedings of the ICP
PW'03, 2003; SUGENG, Hubert; POOL, Jesse: Man-in-the-Middle: Vulnerabilities in Public-key/SSH.Carleton,University, April 2005;

(54) Bezeichnung: **Verfahren zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket**

(57) Hauptanspruch: Verfahren zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket, insbesondere eines Man-In-The-Middle-Angriffs, bei einer Übertragung des Datenpaketes zwischen einem Sender-Knotenpunkt und einem Empfänger-Knotenpunkt in einem paketbasierten Netzwerk aus mehreren, den Sender-Knotenpunkt und den Empfänger-Knotenpunkt umfassenden Knotenpunkten, wobei das Verfahren die folgenden Verfahrensschritte umfaßt:
a) Auslesen von Header-Informationen des Datenpaketes;
b) Ermitteln mindestens eines Parameters aus den ausgelesenen Header-Informationen des Datenpakets;
c) Vergleichen des mindestens einen ermittelten Parameters mit Eintragungen des Sender-Knotenpunktes des Datenpakets in einer Kontrolltabelle, in welcher für alle Knotenpunkte des paketbasierten Netzwerkes jeweils mindestens ein Referenzparameter abgelegt ist; und
d) Feststellen eines unerwünschten Zugriffs auf das Datenpaket, wenn der mindestens eine ermittelte Parameter mit dem entsprechenden mindestens einen Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt.
Wenn ein unerwünschter Zugriff auf das Datenpaket festgestellt wurde:
e) Vergleichen von mindestens einem weiteren ermittelten Parameter mit den Eintragungen in der Kontrolltabelle;...



Beschreibung

[0001] Die Erfindung liegt auf dem Gebiet von Verfahren und Vorrichtungen zum Ermitteln von unerwünschten Zugriffen auf Daten in Datennetzwerken.

Stand der Technik

[0002] Um Daten in einem Datennetzwerk auszuspionieren, bedienen sich Angreifer unterschiedlicher Angriffs-Techniken. Eine dieser Angriffs-Techniken, welche sehr häufig angewendet wird, wird als Man-In-The-Middle-Angriff (MitM-Angriff) bezeichnet. Man-In-The-Middle-Angriffe werden von Angreifern genutzt, um in dem Datennetzwerk auf Daten zuzugreifen, zu denen sie eigentlich keinen Zugriff hätten. Bei derartigen Angriffen wird der Weg der Daten im Datennetzwerk so manipuliert, daß er über die Position des Angreifers im Datennetzwerk führt. Anders ausgedrückt: Der Angreifer wird im Datennetzwerk zwischen Sender und Empfänger positioniert. Diese Position wird MitM-Position genannt.

[0003] Angriffstechniken, um die MitM-Position zu erlangen sind beispielsweise MAC- und ARP-Spoofing, ICMP-Redirects, DHCP-Starvation sowie Spanning-Tree- oder VLAN-Attacken.

[0004] Sicherheitssysteme, welche sich bislang mit dieser Thematik beschäftigen, arbeiten mit Angriffsmuster-Erkennungen. Das bedeutet, daß diese Sicherheitssysteme an Stellen im Netzwerk plaziert werden, die am Entstehungsort diverser Angriffspakete sind, die vom Angreifer in das Netzwerk geschickt werden, um die MitM-Position zu erlangen. Beispiele für Stellen, an denen MitM-Angriffe von gegenwärtig vorhandenen Sicherheitssystemen, wie beispielsweise Network-Intrusion-Detection-Systems (NIDS) aufgespürt werden, sind Switches, Hubs, WLAN-Zugangsknoten, Router und ähnliche aktive Netzwerkkomponenten, die eine Funktion zur Überwachung des aktuellen Datenstroms bieten. Dies ist sehr kostspielig, da die genannten aktiven Netzwerkkomponenten mit den Sicherheitssystemen nachgerüstet werden müssen, um einen Angriff zu erkennen.

[0005] Die Angriffsmuster-Erkennungen basieren beispielsweise auf dem Vergleichen eines aktuellen Datenpaketes mit in einer Datenbank abgelegten Signaturen, die bekannte Angriffe identifizieren. Stimmt das aktuelle Datenpaket mit einer Signatur aus der Datenbank überein, wird ein Angriff gemeldet.

[0006] Ein Sicherheitssystem, welches auf Angriffsmuster-Erkennung basiert, hat weiterhin den Nachteil, daß für jede einzelne dieser Angriffs-Techniken in einer Datenbank eine Art Kontrolldatensatz mit einer Signatur vorhanden sein muß, die es dem Sicherheitssystem erlaubt, den Angriff zu erkennen. Die Datenbank müßte zudem regelmäßig aktualisiert werden, um die neuesten Signaturen für Angriffe zu enthalten.

[0007] Das Dokument US 2005/022020 A1 offenbart ein Authentisierungsprotokoll zum Authentisieren eines Clients, welcher auf einen Server zugreifen will. Mit Hilfe des Authentisierungsprotokolls soll ein Man-in-the-Middle-Angriff (MITM-Angriff) auf den Server verhindert werden. Um das bekannte Authentifizierungsprotokoll einzuleiten, wird von dem Client zunächst eine Authentifizierungsanfrage, welche einen Benutzernamen umfaßt, an den Server übermittelt. Der Server sendet dann einen sogenannten Nonce-Wert an den Client. Aus diesem Nonce-Wert sowie aus anderen Werten ermittelt der Client mittels eines Hash-Algorithmus einen Authentifizierungscode, welchen er an den Server übersendet. Mit Hilfe des gleichen Hash-Algorithmus und der Daten, die auch ihm zur Verfügung stehen, ermittelt der Server einen Vergleichs-Authentifizierungscode. Dieser wird mit dem von dem Client erhaltenen Authentifizierungscode verglichen.

[0008] Die Dokumente US 2003/145232 A1 und US 2002/0311347 A1 beschreiben jeweils ein Verfahren, bei dem in einem Netzwerk übertragene Datenpakete untersucht werden, um einen sogenannten Denial-of-Service-Angriff (DoS-Angriff) zu erkennen und abzuwähren. Hierzu werden aus Header-Informationen der Datenpakete Parameter ermittelt, beispielsweise ein TTL-Wert. Aus den ermittelten Parametern aus mehreren Datenpaketen wird anschließend ein Histogramm erstellt, welches die Häufigkeit anzeigt, mit der die unterschiedlichen Parameter auftreten.

[0009] Das Dokument SUGENG, Hubert; POOL, Jesse: Man-in-the-Middle: Vulnerabilities in Publickey-/SSH (Carleton University, April 2005) beschreibt die Möglichkeit von Man-in-the-Middle-Angriffen gegen Public-Key-Infrastrukturen am Beispiel eines MitM-Angriffs gegen das SSH-Protokoll.

[0010] Das Dokument US 2002/0073338 A1 beschreibt ein System und ein Verfahren zur Eingrenzung von unerwünschtem Verhalten von Computern in Netzwerken.

Die Erfindung

[0011] Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Verfügung zu stellen, welche ein einfaches und zuverlässiges Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket in einem paketbasierten Netzwerk erlauben.

[0012] Die Aufgabe wird erfindungsgemäß durch ein Verfahren nach dem unabhängigen Anspruch 1 und eine Vorrichtung nach dem unabhängigen Anspruch 8 gelöst.

[0013] Erfindungsgemäß ist ein Verfahren zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket, insbesondere eines Man-In-The-Middle-Angriffs, bei einer Übertragung des Datenpaketes zwischen einem Sender-Knotenpunkt und einem Empfänger-Knotenpunkt in einem paketbasierten Netzwerk aus mehreren, den Sender-Knotenpunkt und den Empfänger-Knotenpunkt umfassenden Knotenpunkten, wobei in dem Verfahren Header-Informationen des Datenpaketes ausgelesen werden; mindestens ein Parameter aus den ausgelesenen Header-Informationen des Datenpakets ermittelt wird; der mindestens eine ermittelte Parameter mit Eintragungen des Sender-Knotenpunktes des Datenpakets in einer Kontrolltabelle verglichen wird, in welcher für alle Knotenpunkte des paketbasierten Netzwerkes jeweils mindestens ein Referenzparameter abgelegt ist; und ein unerwünschter Zugriff auf das Datenpaket festgestellt wird, wenn der mindestens eine ermittelte Parameter mit dem entsprechenden mindestens einen Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt.

[0014] Wenn ein unerwünschter Zugriff auf das Datenpaket festgestellt wurde:
In dem Verfahren wird mindestens ein weiterer ermittelter Parameter mit den Eintragungen in der Kontrolltabelle verglichen und ein unerwünschter Zugriff auf das Datenpaket wird als ein unerwünschter Zugriff erster Art identifiziert wird, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle übereinstimmt; und der unerwünschte Zugriff auf das Datenpaket als ein unerwünschter Zugriff zweiter Art identifiziert wird, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt;
wobei in dem Verfahren der für jeden Knotenpunkt in der Kontrolltabelle abgelegte mindestens eine Referenzparameter einen Standard-Time-To-Live-Parameter umfaßt und der mindestens eine ermittelte Parameter einen Time-To-Live-Parameter umfasst, wobei einer der mindestens eine weitere Referenzparameter eine Hardwareadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Hardwareadresse des Sender-Knotenpunktes umfasst; und einer der mindestens eine weitere Referenzparameter eine Netzwerkadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Netzwerkadresse des Sender-Knotenpunktes umfasst; wobei in dem Verfahren die Kontrolltabelle mittels Aussenden von Test-Datenpaketen an den Vermittlungs-Knotenpunkt von allen übrigen der mehreren Knotenpunkte des Netzwerkes und anschließendem Auslesen der Header-Informationen aller Test-Datenpakete zum Ermitteln der Referenzparameter erstellt wird.

[0015] Gegenüber dem Stand der Technik hat das Verfahren den Vorteil, daß die Feststellung des unerwünschten Zugriffs mittels eines einfachen Vergleichs von Parametern mit Referenzparametern erfolgt. Ein Durchsuchen des Datenpakets nach bestimmten Signaturen eines Angriffs muß nicht erfolgen. Dies ermöglicht ein schnelles und zuverlässiges Überprüfen des Datenpakets.

[0016] Außerdem entfällt die Speicherung von Signaturen bekannter Angriffe, die dann mit dem Inhalt des Datenpakets verglichen werden muß. Statt dessen reicht ein Erkennen der Auswirkungen des Angriffs, nämlich der Veränderung von Parametern in den Header-Informationen des Datenpakets, aus, um einen MitM-Angriff festzustellen. Da diese Auswirkungen des Angriffs als Symptome des Angriffs anzusehen sind, kann hier von einer symptomatischen Erkennung eines MitM-Angriffs gesprochen werden. Hierdurch werden auch Angriffe, deren Art bislang unbekannt sind, die aber eine Positionierung des Angreifers in einer MitM-Position zur Folge haben, durch die im erfindungsgemäßen Verfahren untersuchten Symptome erkannt.

[0017] Ferner kann ein Angriff auch an einer Stelle im Netz ermittelt, die sich nicht unmittelbar am Ursprungsort des Angriffs, also an der Position im paketbasierten Netzwerk, an der ein Rechner des Angreifers tatsächlich angeschlossen ist, befindet. Somit werden keine aufwendigen Anforderungen an das paketbasierte Netzwerk gestellt, wie beispielsweise eine Überwachungsfunktion aktiver Knotenpunkte, wie Hubs oder Switches.

[0018] Weitere Vorteile von bevorzugten Ausführungsformen der Erfindung sind Gegenstand der abhängigen Ansprüche.

[0019] Erfindungsgemäß ist ferner eine Vorrichtung zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket, insbesondere eines Man-In-The-Middle-Angriffs, bei einer Übertragung des Datenpaketes zwischen einem Sender-Knotenpunkt und einem Empfänger-Knotenpunkt in einem paketbasierten Netzwerk aus mehreren, den Sender-Knotenpunkt und den Empfänger-Knotenpunkt umfassenden Knotenpunkten vorgesehen, wobei die Vorrichtung Verbindungsmittel zum Verbinden mit dem paketbasierten Netzwerk; Empfangsmittel zum Empfangen des Datenpakets; Auslesemittel zum Auslesen von Header-Informationen des Datenpaketes; Extraktionsmittel zum Ermitteln mindestens eines Parameters aus den ausgelesenen Header-Informationen des Datenpakets; Speichermittel zum Speichern einer Kontrolltabelle, in welcher für alle Knotenpunkte des paketbasierten Netzwerkes jeweils mindestens ein Refe-

renzparameter abgelegt ist; Vergleichsmittel zum Vergleichen des mindestens einen ermittelten Parameters mit Eintragungen in der in den Speichermittel gespeicherten Kontrolltabelle; Verarbeitungsmittel zum Feststellen eines unerwünschten Zugriffs auf das Datenpaket, wenn der mindestens eine ermittelte Parameter für keines der Knotenpunkte mit dem entsprechenden mindestens einen Referenzparameter in der Kontrolltabelle übereinstimmt; und Mittel zum Vergleichen von mindestens einem weiteren ermittelten Parameter mit den Eintragungen in der Kontrolltabelle; und Mittel zum Identifizieren des unerwünschten Zugriffs auf das Datenpaket als einen unerwünschten Zugriff erster Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle übereinstimmt; und Mittel zum Identifizieren des unerwünschten Zugriffs auf das Datenpaket als einen unerwünschten Zugriff zweiter Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt; wobei der für jeden Knotenpunkt in der Kontrolltabelle abgelegte mindestens eine Referenzparameter einen Standard-Time-To-Live-Parameter umfaßt und der mindestens eine ermittelte Parameter einen Time-To-Live-Parameter umfasst, wobei einer der mindestens eine weitere Referenzparameter eine Hardwareadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Hardwareadresse des Sender-Knotenpunktes umfasst; und einer der mindestens eine weitere Referenzparameter eine Netzwerkadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Netzwerkadresse des Sender-Knotenpunktes umfasst, wobei die Kontrolltabelle mittels Aussenden von Test-Datenpaketen an den Vermittlungs-Knotenpunkt von allen übrigen der mehreren Knotenpunkte des Netzwerkes und anschließendem Auslesen der Header-Informationen aller Test-Datenpakete zum Ermitteln der Referenzparameter erstellt wird; und Sendemittel zum Weiterleiten des Datenpakets umfaßt.

Beschreibung von bevorzugten Ausführungsbeispielen

[0020] Die Erfindung wird im folgenden anhand von Ausführungsbeispielen unter Bezugnahme auf Figuren einer Zeichnung näher erläutert. Hierbei zeigen:

[0021] Fig. 1 eine schematische Darstellung eines paketbasierten Netzwerkes mit einem Rechner A und einem Rechner B;

[0022] Fig. 2 eine schematische Darstellung einer Übertragung eines Datenpaketes;

[0023] Fig. 3 eine schematische Darstellung eines Abschnittes eines Datenpaketes mit Nutzdaten und Header-Informationen;

[0024] Fig. 4 einen Ablauf-Diagramm der Übertragung eines Datenpaketes zwischen einem Rechner A und einem Rechner B;

[0025] Fig. 5 eine schematische Darstellung eines weiteren paketbasierten Netzwerkes mit einem Rechner A, einem Rechner B und einem Angreifer;

[0026] Fig. 6 ein Ablauf-Diagramm einer Übertragung eines Datenpaketes, bei der ein Angriff basierend auf einer erste Methode erfolgt;

[0027] Fig. 7 ein Ablauf-Diagramm einer Übertragung eines Datenpaketes, bei der ein Angriff basierend auf einer zweite Methode erfolgt;

[0028] Fig. 8 ein weiteres paketbasiertes Netzwerk mit einem Rechner A, einem Rechner B, einem Angreifer und einer Vorrichtung zum Ermitteln eines unerwünschten Zugriffs;

[0029] Fig. 9 einen Aufbau einer Kontrolltabelle;

[0030] Fig. 10 ein Ablauf-Diagramm eines Verfahrens zum Ermitteln eines Angriffs auf ein Datenpaket; und

[0031] Fig. 11 ein Ablauf-Diagramm eines weiteren Verfahrens zum Ermitteln eines Angriffs auf ein Datenpaket.

[0032] Fig. 1 zeigt eine schematische Darstellung eines paketbasierten Netzwerkes, welches zwei Knotenpunkte umfaßt. In dem hier gezeigten paketbasierten Netzwerk soll ein Datenpaket von einem Sender-Knotenpunkt, und einem Empfänger-Knotenpunkt übertragen werden. Der Sender-Knotenpunkt wird durch einen Rechner A gebildet, während der Empfänger-Knotenpunkt durch einen Rechner B gebildet wird.

[0033] Hierbei werden die Knotenpunkte des paketbasierten Netzwerkes mittels zweier Parameter gekennzeichnet. Einer dieser Parameter ist die sogenannte MAC-Adresse (MAC – „Media Access Control") des Knotenpunktes. Eine MAC-Adresse ist eine Hardwareadresse, welche einem Netzwerkelement, beispielsweise einer Netzwerkkarte in einem Rechner, bei seiner Herstellung zugeordnet wird. Jeder Hersteller von Netzwerkelementen hat einen bestimmten Anfangswert, mit dem jede Hardwareadresse der von ihm hergestellten Netzwerkelemente beginnt. Die Hardwareadresse kennzeichnet das Netzwerkelement eindeutig und ist mittels Software nicht veränderbar. Der andere der zwei Parameter zur Kennzeichnung eines Knotenpunktes ist die so-

genannte IP-Adresse (IP – „Internet Protocol"). Die IP-Adresse ist eine Netzwerkadresse, welche einem Knotenpunkt in einem paketbasierten Netzwerk beim Anmelden des Knotenpunktes softwaremäßig zugeordnet wird. Wenn das paketbasierte Netzwerk ein Teilnetzwerk eines größeren Gesamtnetzwerkes ist, kann es sich bei der einem Knotenpunkt des paketbasierten Netzwerkes zugeordneten IP-Adresse um eine private IP-Adresse handeln, welche den Knotenpunkt in dem Gesamtnetzwerk nicht eindeutig kennzeichnet.

[0034] In dem in der Fig. 1 gezeigten Netzwerk sind der Einfachheit halber der Rechner A und der Rechner B direkt, das heißt ohne das Vorhandensein eines dazwischenliegenden Knotenpunktes, miteinander verbunden. Im Allgemeinen werden Datenpakete jedoch für die Übertragung von Daten in größeren Netzwerken verwendet. In diesen Fällen muß ein Datenpaket typischerweise mehrere zwischen dem Sender-Knotenpunkt und dem Empfänger-Knotenpunkt angeordnete Knotenpunkte passieren. Hierbei können die das Netzwerk bildenden Knotenpunkte beispielsweise Router, Switches und ähnliche Vorrichtungen umfassen.

[0035] Die Fig. 2 veranschaulicht den Ablauf einer Übertragung eines Nutzdaten umfassenden Datenpaketes vom Rechner A zum Rechner B. Hierzu wird zunächst das Datenpaket im Rechner A gebildet, indem den Nutzdaten mittels eines Übertragungsprotokolls, beispielsweise des im Internet verwendeten TCP/IP-Protokolls, wichtige Informationen angehängt werden, beispielsweise über die zu übertragenden Nutzdaten, dem Rechner A, dem Format, mittels welchem die Nutzdaten kodiert sind, usw. Diese Informationen werden in einem Abschnitt zusammengefaßt, welcher im Allgemeinen den Anfang oder Kopf eines Datenpakets bildet.

[0036] Dieser Abschnitt wird daher auch Protokoll-Kopf oder Header genannt, wobei die hierin enthaltenen Informationen als Header-Informationen bezeichnet werden. Der Vorgang des Bildens des Datenpakets im Rechner A ist in der Fig. 2 mittels des Pfeils A veranschaulicht. Das Übertragungsprotokoll umfaßt unterschiedliche Schichten („Layers"). In jedem dieser Schichten werden die Nutzdaten mit einem eigenen Header versehen. In dem hier dargestellten Übertragungsprotokoll umfaßt das sogenannte ISO OSI-Schichtenmodell fünf Schichten. Andere Übertragungsprotokolle können mehr oder weniger Schichten umfassen.

[0037] Wie mittels des Pfeils B in der Fig. 2 dargestellt, kann das Datenpaket anschließend zum Rechner B übertragen werden. Am Rechner B angekommen, muß das Datenpaket dann die verschiedenen Schichten des Übertragungsprotokolls in umgekehrter Reihenfolge durchlaufen. Dies wird mit Hilfe des Pfeils C in der Fig. 2 angedeutet. Hierbei werden die zuvor im Rechner A hinzugefügten Header-Informationen schrittweise vom Datenpaket entfernt und ausgewertet, so daß dem Rechner B schließlich die Nutzdaten zur Verfügung stehen.

[0038] Die Fig. 3 zeigt eine schematische Darstellung eines Abschnittes des Datenpaketes, um den Aufbau des Datenpaketes zu verdeutlichen. Das Datenpaket umfaßt Nutzdaten und Header-Informationen. Die Header-Informationen umfassen Informationen und Parameter, welche für die korrekte Übertragung und anschließende Bearbeitung des Datenpaketes benötigt werden. In der Fig. 3 sind beispielhaft Parameter dargestellt, welche von den Headern umfaßt werden, die den Nutzdaten von der Schicht **2** (Data Link Layer) und der Schicht **3** (Transport Layer) des in der Fig. 2 dargestellten Übertragungsprotokolls hinzugefügt wurden. Die Nutzdaten werden in der Schicht **3** (Transport Layer) mit einem IP-Header versehen. Der IP-Header dient zu Routing-Zwecken in IP-Netzwerken. IP-Header umfassen daher die IP-Adresse des Empfänger-Knotenpunktes (IP-Ziel-Adresse) und die IP-Adresse des Sender-Knotenpunktes (IP-Quell-Adresse), sowie einen sogenannten Time-To-Live-Parameter (TTL-Parameter). Weiterhin umfassen die Header-Informationen die MAC-Adresse des Sender-Knotenpunktes (MAC-Quell-Adresse) und die MAC-Adresse des Empfänger-Knotenpunktes (MAC-Ziel-Adresse). Der TTL-Parameter bestimmt die Anzahl der Knotenpunkte, die das Datenpaket durchlaufen kann, bevor es verworfen wird. Zweck des TTL-Parameter ist es beispielsweise, Endlosschleifen von Datenpaketen zu vermeiden.

[0039] Ein TTL-Anfangswert, das heißt der Wert des TTL-Parameter zu Beginn der Übertragung des Datenpaketes, ist vom Betriebsystem abhängig, welches vom Sender-Knotenpunkt verwendet wird. Der TTL-Anfangswert variiert typischerweise zwischen 32 und 255. Beispielsweise verwendet ein Linux-Betriebssystem typischerweise einen TTL-Anfangswert von 64. Der TTL-Parameter wird um jeweils 1 herabgesetzt, sobald das Datenpaket einen weiteren Knotenpunkt, welcher beispielsweise einen weiteren Rechners, einen Router oder ähnliches passiert.

[0040] Die Fig. 4 zeigt ein Ablauf-Diagramm, welches die Übertragung eines Datenpaketes zwischen dem Rechner A und Rechner B veranschaulicht. Hierbei wird zunächst das Datenpaket im Rechner A erzeugt (Schritt **1**). Anschließend wird das Datenpaket vom Rechner A ausgesendet (Schritt **2**). Das Datenpaket wird schließlich vom Rechner B empfangen (Schritt **3**). Wie in der Fig. 4 dargestellt, wird das Datenpaket mit einem im Rechner A mit einem TTL-Anfangswert von 64 versehen. Da das Datenpaket bei der hier dargestellten Übertragung zwischen dem Rechner A und dem Rechner B keinen weiteren Kno-

tenpunkt durchlauft, bleibt der Wert des TTL-Parameter beim Empfang des Datenpaketes unverändert bei 64. Auch die weiteren hier dargestellten, die Header-Informationen bildenden Parameter, nämlich die MAC-Ziel-Adresse, die IP-Ziel-Adresse, die MAC-Quell-Adresse und die IP-Quell-Adresse bleiben bei der Übertragung unverändert.

[0041] Die Fig. 5 zeigt ein weiteres paketbasiertes Netzwerk aus einem Rechner A als Sender-Knotenpunkt und einem Rechner B als Empfänger-Knotenpunkt. Zusätzlich hierzu umfaßt das weitere paketbasierte Netzwerk auch einen Angreifer, welcher sich zwischen dem Rechner A und dem Rechner B positioniert hat, um auf ein vom Rechner A zum Rechner B zu übertragendes Datenpaket zuzugreifen. Bei dem Angreifer kann es sich beispielsweise um einen einfachen Rechner handeln, der mit dem paketbasierten Netzwerk aus der Fig. 1 verbunden wurde, um etwa sensible Daten abzugreifen und/oder zu manipulieren. In diesem Fall spricht man davon, daß sich der Angreifer in die MitM-Position zwischen Rechner A und Rechner B bringt.

[0042] In dem vorliegenden Beispiel hat der Rechner A die MAC-Adresse 00:00:00:00:00:01 und die IP-Adresse 10.0.0.1, während der Rechner B die MAC-Adresse 00:00:00:00:00:05 und die IP-Adresse 10.0.0.5 aufweist. Der Angreifer weist die MAC-Adresse 00:00:00:00:00:02 und die IP-Adresse 10.0.0.2 auf.

[0043] Die Fig. 6 zeigt ein Ablauf-Diagramm der Übertragung eines Datenpaketes in dem paketbasierten Netzwerk aus der Fig. 5. Auch hier wird zunächst das Datenpaket im Rechner A erzeugt (Schritt **4**) und anschließend vom Rechner A versendet (Schritt **5**). Nun kommt jedoch der Angreifer, welcher sich zwischen den Rechnern A und B positioniert hat zum Zug und empfängt das Datenpaket (Schritt **6**). Das Datenpaket wird anschließend vom Angreifer modifiziert (Schritt **7**) und wieder versendet (Schritt **8**), so daß es schließlich vom Rechner B empfangen wird (Schritt **9**).

[0044] Wenn sich der Angreifer einmal in seiner MitM-Position positioniert und auf ein Datenpaket zugegriffen hat, kann er im Allgemeinen eine von zwei Methoden anwenden, um das Datenpakete weiterzuleiten. Eine erste Methode wird „Forwarding" genannt und ist in dem Diagramm in Fig. 6 dargestellt. Bei dieser Methode bleibt die IP-Quell-Adresse des Datenpaketes erhalten, es ändert sich jedoch die MAC-Quell-Adresse. Anstatt der MAC-Adresse des Rechners A wird nun die MAC-Adresse des Angreifers im Ethernet-Header eingetragen.

[0045] Wie in der Fig. 6 zu erkennen ist, wurden durch das „Forwarding" die Parameter des Datenpaketes vom Angreifer dahingehend modifiziert, daß es zum einen nun die MAC-Quell-Adresse des Angreifers enthält (00:00:00:00:00:02), und zum anderen wurde der Time-To-Live-Wert (TTL) des Paketes um 1 vermindert (von 64 auf 63). Das Wesentliche hierbei ist jedoch, dass die IP-Quell-Adresse als die IP-Adresse des Rechners A (10.0.0.1) beibehalten wird, während MAC-Quell-Adresse geändert wird, so daß sie mit der MAC-Adresse des Angreifers übereinstimmt. Hierdurch entsteht eine Inkonsistenz zwischen der IP-Quell-Adresse und der MAC-Quell-Adresse in den Header-Informationen des Datenpaketes. Das bedeutet, die IP-Quell-Adresse und die MAC-Quell-Adresse stimmen nicht mit einem Paar von IP-Adresse und MAC-Adresse eines Knotenpunktes im paketbasierten Netzwerk überein.

[0046] Eine zweite Methode ist die so genannte „NAT" (Network-Address-Translation), welche in der Fig. 7 veranschaulicht wird. Hierbei wird ähnlich wie in der Fig. 6 ebenfalls ein vom Rechner A generiertes (Schritt **10**) und versendetes (Schritt **11**) Datenpaket von einem zwischen den Rechnern A und B positionierten Angreifer empfangen (Schritt **12**). Das Datenpaket wird anschließend vom Angreifer modifiziert (Schritt **13**) und wieder versendet (Schritt **14**), so daß es schließlich vom Rechner B empfangen wird (Schritt **15**). Bei dem auf NAT basierenden Angriff wird jedoch, im Gegensatz zu dem auf Forwarding basierenden Angriff, sowohl die IP-Quell-Adresse als auch die MAC-Quell-Adresse des Datenpaketes vom Angreifer modifiziert. Das bedeutet, die Header-Informationen des vom Rechner B im Schritt **15** empfangenen Datenpaketes umfassen eine IP-Quell-Adresse und eine MAC-Quell-Adresse, welche nicht mehr mit der IP-Adresse und der MAC-Adresse des Rechners A sondern mit der IP-Adresse und der MAC-Adresse des Angreifers übereinstimmen.

[0047] Nun sind die IP-Quell-Adresse und die MAC-Quell-Adresse konsistent. Das bedeutet, die IP-Quell-Adresse und die MAC-Quell-Adresse stimmen mit der IP-Adresse und der MAC-Adresse eines Knotenpunktes, nämlich des Angreifers, im paketbasierten Netzwerk überein. Deshalb würde in diesem Fall eine Überprüfung der IP-Quell-Adresse und der MAC-Quell-Adresse allein nicht ausreichen, um einen unerwünschten Zugriff auf das Datenpaket zu ermitteln.

[0048] Jedoch wird auch in diesem Fall, der TTL-Parameter um 1 vermindert (von 63 auf 64), da das Datenpaket einen Knotenpunkt, nämlich den Angreifer, passiert hat. Das führt dazu, daß der TTL-Parameter einen Wert aufweist, der von dem Wert abweicht, den der TTL-Parameter aufgewiesen hätte, hätte der Angreifer das Datenpaket nicht empfangen und wieder versendet.

[0049] Die Fig. 8 zeigt ein paketbasiertes Netzwerk

mit dem Rechner A, dem Rechner B, dem Angreifer sowie einer vor dem Rechner B geschalteten sogenannten MitM-Bridge. Die MitM-Bridge umfaßt eine Vorrichtung zum Ermitteln eines unerwünschten Zugriffs auf ein zwischen dem Rechner A und dem Rechner B übertragenes Datenpaket. Die MitM-Bridge bildet in diesem Fall einen Knotenpunkt im paketbasierten Netzwerk. In einer anderen Ausführung kann der MitM-Bridge jedoch auch einen Teil des Rechners B bilden. Wenn das paketbasierte Netzwerk ein Teilnetz eines übergeordneten Gesamtnetzwerkes, beispielsweise des Internets, ist und über sogenannte Gateways mit Knotenpunkten des Gesamtnetzwerkes verbunden ist, kann die MitM-Bridge zweckmäßigerweise vor einem der Gateways angeordnet werden, um eine Übertragung von Datenpaketen zwischen einem Knotenpunkt des paketbasierten Netzwerkes und einem Knotenpunkt des Gesamtnetzwerkes außerhalb des paketbasierten Netzwerkes zu überprüfen.

[0050] Vorteilhaft ist auch ein Positionieren der MitM-Bridge vor sensiblen Systemen, wie Datenbank-Servern, Datei-Servern oder ähnlichen Systemen im paketbasierten Netzwerk, die vor Passwort-Diebstahl zu schützen sind.

[0051] Die Fig. 9 zeigt schematisch eine Kontrolltabelle, welche Eintragungen für jeden Knotenpunkt im paketbasierten Netzwerk umfaßt. In der Kontrolltabelle sind für jeden Knotenpunkt die MAC-Adresse sowie die IP-Adresse des Knotenpunktes abgelegt. Diese Adressen können zum Beispiel von einem Netzwerkverwalter zur Verfügung gestellt worden sein, welcher die Adressen zur Verwaltung von Datenpaket-Übertragungen im paketbasierten Netzwerk benötigt. Wenn sich beispielsweise weitere Rechner als weitere Knotenpunkte mit dem paketbasierten Netzwerk verbinden möchten, so werden zunächst die MAC-Adresse sowie die IP-Adresse dieser weiteren Rechner der Kontrolltabelle hinzugefügt.

[0052] Vorteilhafterweise ist die Kontrolltabelle in einem Speicher der MitM-Bridge gespeichert.

[0053] Für jedem Knotenpunkt umfaßt die Kontrolltabelle ferner einen sogenannten Standard-TTL-Parameter. Dies ist der TTL-Parameter, welchen ein Datenpaket aufweist, der von dem jeweiligen Knotenpunkt abgesendet und von dem Knotenpunkt, an welchem die Kontrolltabelle gespeichert ist, beispielsweise von der MitM-Bridge aus der Fig. 8, empfangen wird, wenn kein Angreifer im paketbasierten Netzwerk vorhanden ist. Der Standard-TTL-Parameter dient somit als ein Referenzparameter.

[0054] Die Fig. 10 zeigt den Ablauf-Diagramm eines Verfahrens zum Ermitteln eines Man-In-The-Middle-Angriffs auf ein Datenpaket in einem paketbasierten Netzwerk. Hierbei werden zunächst die Header-Informationen des Datenpaketes ausgelesen und der TTL-Parameter aus den ausgelesenen Header-Informationen ermittelt (Schritt **20**). Anschließend wird der ermittelte TTL-Parameter mit jedem der in der Kontrolltabelle gespeicherten Standard-TTL-Parameter verglichen (Schritt **21**). Wird ein mit dem TTL-Parameter übereinstimmender Standard-TTL-Parameter gefunden, so wird angenommen, daß der zu dem Standard-TTL-Parameter gehörende Knotenpunkt das Datenpaket ausgesendet hat, und das Datenpaket wird weitergeleitet (Schritt **22**). Sollte jedoch der TTL-Parameter mit keinem der in der Kontrolltabelle gespeicherten Standard-TTL-Parameter übereinstimmen, so ist dies ein Anzeichen dafür, daß ein MitM-Angriff stattgefunden hat und auf das Datenpaket unerwünscht zugegriffen worden ist.

[0055] In diesem Fall wird anhand eines Vergleiches der IP-Adresse und der MAC-Adresse mit den Eintragungen in der Kontrolltabelle überprüft, um welche Art eines MitM-Angriff es sich handelt (Schritt **23**). Dieser zusätzliche Vergleichsschritt kann jedoch in einer vereinfachten Ausführungsform des Verfahrens entfallen.

[0056] Stellt sich bei dem Vergleich heraus, daß die IP-Quell-Adresse und die MAC-Quell-Adresse des Datenpaketes konsistent sind, das bedeutet, es wird ein mit diesen Adressen übereinstimmendes Paar an IP-Adresse und MAC-Adresse in der Kontrolltabelle gefunden, so handelt es sich bei dem MitM-Angriff um einen auf NAT basierenden Angriff, einen sogenannten NATed-MitM. Es wird anschließend ein Warnhinweis erzeugt, um den Angriff anzuzeigen (Schritt **24**).

[0057] Bei einem NATed-MitM kann der entsprechende Knotenpunkt, dessen IP-Adresse und MAC-Adresse mit der IP-Quell-Adresse und der MAC-Quell-Adresse des Datenpaketes, auf welches unerwünscht zugegriffen wurde, aus dem paketbasierten Netzwerk isoliert werden.

[0058] Sind jedoch die IP-Quell-Adresse und die MAC-Quell-Adresse des Datenpaketes inkonsistent, das heißt, das paketbasierte Netzwerk umfaßt keinen Knotenpunkt mit dem entsprechenden Paar von IP-Adresse und MAC-Adresse, so handelt es sich bei dem MitM-Angriff um einen auf Forwarding basierenden Angriff, einen sogenannten Forwarded-MitM, und ein entsprechender Warnhinweis wird erzeugt (Schritt **25**).

[0059] Die Fig. 11 zeigt den Ablauf-Diagramm eines weiteren Verfahrens zum Ermitteln eines Man-In-The-Middle-Angriffs auf ein Datenpaket in einem paketbasierten Netzwerk. Hierbei werden ebenso wie im vorangehend beschriebenen Verfahren die Header-Informationen des Datenpaketes ausgelesen

und der TTL-Parameter aus den ausgelesenen Header-Informationen ermittelt (Schritt **30**). Anschließend wird der ermittelte TTL-Parameter mit jedem der in der Kontrolltabelle gespeicherten Standard-TTL-Parameter verglichen (Schritt **31**). Wird ein mit dem TTL-Parameter übereinstimmender Standard-TTL-Parameter entdeckt, so wird in diesem Fall nicht sofort angenommen, daß der zu dem Standard-TTL-Parameter gehörende Knotenpunkt das Datenpaket ausgesendet hat. Statt dessen werden die beiden anderen Parameter, nämlich die IP-Quell-Adresse und die MAC-Quell-Adresse des Datenpaketes mit der IP-Adresse und der MAC-Adresse des entsprechenden Knotenpunktes in der Kontrolltabelle verglichen. Nur wenn alle drei Parameter des Datenpaketes, nämlich der TTL-Parameter, die IP-Quell-Adresse und die MAC-Quell-Adresse, eine Entsprechung in der Kontrolltabelle finden, kann angenommen werden, daß auf das Datenpaket nicht unerwünscht zugegriffen wurde, und das Datenpaket kann weitergeleitet werden (Schritt **35**).

[0060] Sollte anhand der Kontrolltabelle eine Inkonsistenz zwischen der IP-Quell-Adresse und der MAC-Quell-Adresse ermittelt worden sein, so ist es möglich, daß eine bisher unbekannte Art eines MitM-Angriffs stattgefunden hat. In diesem Fall wird eine entsprechende Warnung ausgegeben (Schritt **34**).

[0061] Sollte jedoch der TTL-Parameter mit keinem der in der Kontrolltabelle gespeicherten Standard-TTL-Parameter übereinstimmen, so ist dies analog zu dem Verfahren aus der Fig. 10 ein Anzeichen dafür, daß ein MitM-Angriff stattgefunden hat und auf das Datenpaket unerwünscht zugegriffen worden ist. In diesem Fall wird ebenfalls anhand eines Vergleiches der IP-Adresse und der MAC-Adresse mit den Eintragungen in der Kontrolltabelle überprüft, um welche Art eines MitM-Angriff es sich handelt (Schritt **33**). Dieser zusätzliche Vergleichsschritt kann jedoch in einer vereinfachten Ausführungsform des Verfahrens entfallen.

[0062] Stellt sich bei dem Vergleich heraus, daß die IP-Quell-Adresse und die MAC-Quell-Adresse des Datenpaketes konsistent sind, so handelt es sich bei dem MitM-Angriff um einen auf NAT basierenden Angriff, einen sogenannten NATed-MitM. Es wird anschließend ein Warnhinweis erzeugt, um den Angriff anzuzeigen (Schritt **36**). Sind jedoch die IP-Quell-Adresse und die MAC-Quell-Adresse des Datenpaketes inkonsistent, das heißt, das paketbasierte Netzwerk umfaßt keinen Knotenpunkt mit dem entsprechenden Paar von IP-Adresse und MAC-Adresse, so handelt es sich um einen sogenannten Forwarded-MitM und ein entsprechender Warnhinweis wird erzeugt (Schritt **37**). Alternativ oder zusätzlich kann in diesem Fall der Knotenpunkt, dessen MAC-Adresse mit der MAC-Quell-Adresse des Datenpaketes übereinstimmt, als Knotenpunkt eines Angreifers identifiziert und aus dem Netzwerk isoliert werden.

[0063] Wenn ein MitM-Angriff ermittelt wurde, kann außerdem das betroffene Datenpaket isoliert, beispielsweise gelöscht, werden, um ein weiteres Sicherheitsrisiko für das paketbasierte Netzwerk zu vermeiden.

[0064] Bei den vorangehend beschriebenen Verfahren wurde zunächst oder ausschließlich der TTL-Parameter des Datenpaketes mit den Eintragungen in der Kontrolltabelle verglichen. Es können hierzu jedoch auch zunächst oder ausschließlich die IP-Quell-Adresse und/oder die MAC-Quell-Adresse verwendet werden.

[0065] Die in der vorstehenden Beschreibung, den Ansprüchen und der Zeichnung offenbarten Merkmale der Erfindung können sowohl einzeln als auch in beliebigen Kombinationen für die Verwirklichung der Erfindung in ihren verschiedenen Ausführungsformen von Bedeutung sein.

Patentansprüche

1. Verfahren zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket, insbesondere eines Man-In-The-Middle-Angriffs, bei einer Übertragung des Datenpaketes zwischen einem Sender-Knotenpunkt und einem Empfänger-Knotenpunkt in einem paketbasierten Netzwerk aus mehreren, den Sender-Knotenpunkt und den Empfänger-Knotenpunkt umfassenden Knotenpunkten, wobei das Verfahren die folgenden Verfahrensschritte umfaßt:
a) Auslesen von Header-Informationen des Datenpaketes;
b) Ermitteln mindestens eines Parameters aus den ausgelesenen Header-Informationen des Datenpakets;
c) Vergleichen des mindestens einen ermittelten Parameters mit Eintragungen des Sender-Knotenpunktes des Datenpakets in einer Kontrolltabelle, in welcher für alle Knotenpunkte des paketbasierten Netzwerkes jeweils mindestens ein Referenzparameter abgelegt ist; und
d) Feststellen eines unerwünschten Zugriffs auf das Datenpaket, wenn der mindestens eine ermittelte Parameter mit dem entsprechenden mindestens einen Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt.
Wenn ein unerwünschter Zugriff auf das Datenpaket festgestellt wurde:
e) Vergleichen von mindestens einem weiteren ermittelten Parameter mit den Eintragungen in der Kontrolltabelle;
f) Identifizieren des unerwünschten Zugriffs auf das

Datenpaket als einen unerwünschten Zugriff erster Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle übereinstimmt, und

g) Identifizieren des unerwünschten Zugriffs auf das Datenpaket als einen unerwünschten Zugriff zweiter Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt;

wobei der für jeden Knotenpunkt in der Kontrolltabelle abgelegte mindestens eine Referenzparameter einen Standard-Time-To-Live-Parameter umfaßt und der mindestens eine ermittelte Parameter einen Time-To-Live-Parameter umfasst,

wobei einer der mindestens eine weitere Referenzparameter eine Hardwareadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Hardwareadresse des Sender-Knotenpunktes umfasst; und

einer der mindestens eine weitere Referenzparameter eine Netzwerkadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Netzwerkadresse des Sender-Knotenpunktes umfasst,

wobei die Kontrolltabelle mittels Aussenden von Test-Datenpaketen an den Vermittlungs-Knotenpunkt von allen übrigen der mehreren Knotenpunkte des Netzwerkes und anschließendem Auslesen der Header-Informationen aller Test-Datenpakete zum Ermitteln der Referenzparameter erstellt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Verfahren an einem Vermittlungs-Knotenpunkt durchgeführt wird, welcher zwischen dem Sender-Knotenpunkt und dem Empfänger-Knotenpunkt angeordneten ist oder mit dem Empfänger-Knotenpunkt übereinstimmt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der mindestens eine Knotenpunkt isoliert wird, wenn der unerwünschte Zugriff auf das Datenpaket als ein unerwünschter Zugriff erster Art Identifiziert wurde.

4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Verfahren in jedem Knotenpunkt des paketbasierten Netzwerkes durchgeführt wird.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das paketbasiertes Netzwerk ein Teilnetzwerk eines übergeordneten Gesamtnetzwerk ist.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß ein Warnhinweis angezeigt wird, wenn ein unerwünschter Zugriff auf das Datenpaket festgestellt wurde.

7. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß das Datenpaket gelöscht wird, wenn ein unerwünschter Zugriff auf das Datenpaket festgestellt wurde.

8. Vorrichtung zum Ermitteln eines unerwünschten Zugriffs auf ein Datenpaket, insbesondere eines Man-In-The-Middle-Angriffs, bei einer Übertragung des Datenpaketes zwischen einem Sender-Knotenpunkt und einem Empfänger-Knotenpunkt in einem paketbasierten Netzwerk aus mehreren, den Sender-Knotenpunkt und den Empfänger-Knotenpunkt umfassenden Knotenpunkten, mit:

– Verbindungsmittel zum Verbinden mit dem paketbasierten Netzwerk;

– Empfangsmittel zum Empfangen des Datenpakets;

– Auslesemittel zum Auslesen von Header-Informationen des Datenpaketes;

– Extraktionsmittel zum Ermitteln mindestens eines Parameters aus den ausgelesenen Header-Informationen des Datenpakets;

– Speichermittel zum Speichern einer Kontrolltabelle, in welcher für alle Knotenpunkte des paketbasierten Netzwerkes jeweils mindestens ein Referenzparameter abgelegt ist;

– Vergleichsmittel zum Vergleichen des mindestens einen ermittelten Parameters mit Eintragungen in der in den Speichermittel gespeicherten Kontrolltabelle;

– Verarbeitungsmittel zum Feststellen eines unerwünschten Zugriffs auf das Datenpaket, wenn der mindestens eine ermittelte Parameter für keines der Knotenpunkte mit dem entsprechenden mindestens einen Referenzparameter in der Kontrolltabelle übereinstimmt; und

– Mittel zum Vergleichen von mindestens einem weiteren ermittelten Parameter mit den Eintragungen in der Kontrolltabelle; und

– Mittel zum Identifizieren des unerwünschten Zugriffs auf das Datenpaket als einen unerwünschten Zugriff erster Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle übereinstimmt; und

– Mittel zum Identifizieren des unerwünschten Zugriffs auf das Datenpaket als einen unerwünschten Zugriff zweiter Art, wenn der mindestens eine weitere ermittelte Parameter mit dem entsprechenden mindestens einen weiteren Referenzparameter des Sender-Knotenpunktes des Datenpakets in der Kontrolltabelle nicht übereinstimmt;

wobei der für jeden Knotenpunkt in der Kontrolltabelle abgelegte mindestens eine Referenzparameter einen Standard-Time-To-Live-Parameter umfaßt und der mindestens eine ermittelte Parameter einen Time-To-Live-Parameter umfasst,

wobei einer der mindestens eine weitere Referenz-

parameter eine Hardwareadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Hardwareadresse des Sender-Knotenpunktes umfasst; und
einer der mindestens eine weitere Referenzparameter eine Netzwerkadresse des Knotenpunktes umfaßt und einer der mindestens eine weitere ermittelte Parameter eine Netzwerkadresse des Sender-Knotenpunktes umfasst,
wobei die Kontrolltabelle mittels Aussenden von Test-Datenpaketen an den Vermittlungs-Knotenpunkt von allen übrigen der mehreren Knotenpunkte des Netzwerkes und anschließendem Auslesen der Header-Informationen aller Test-Datenpakete zum Ermitteln der Referenzparameter erstellt wird; und
– Sendemittel zum Weiterleiten des Datenpakets.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

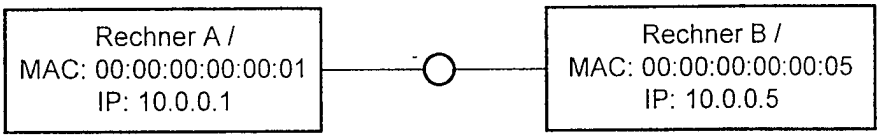


Fig. 1

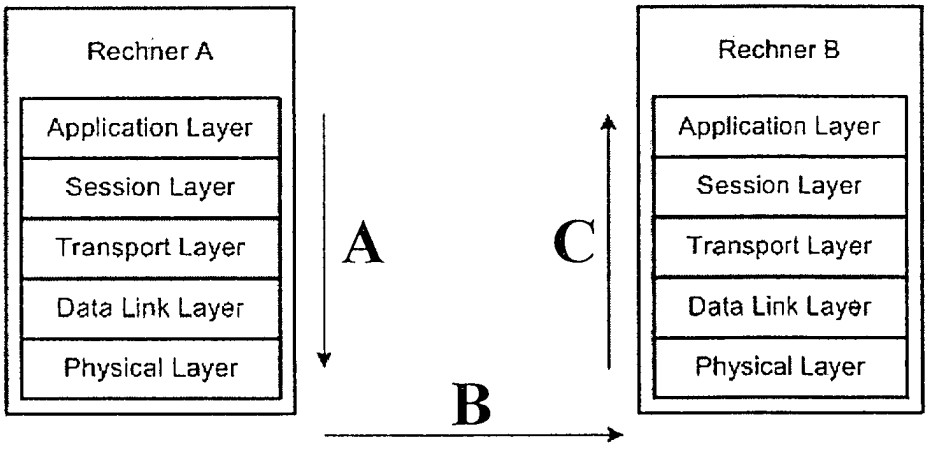


Fig. 2

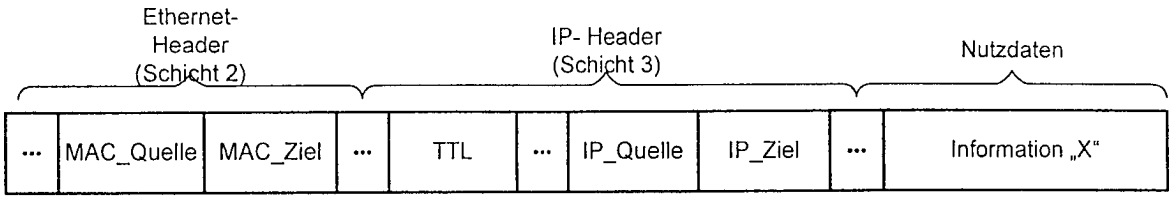

Ethernet-
Header
(Schicht 2)
IP- Header
(Schicht 3)
Nutzdaten
...
MAC_Quelle
MAC_Ziel
...
TTL
...
IP_Quelle
IP_Ziel
...
Information „X“

Fig. 3

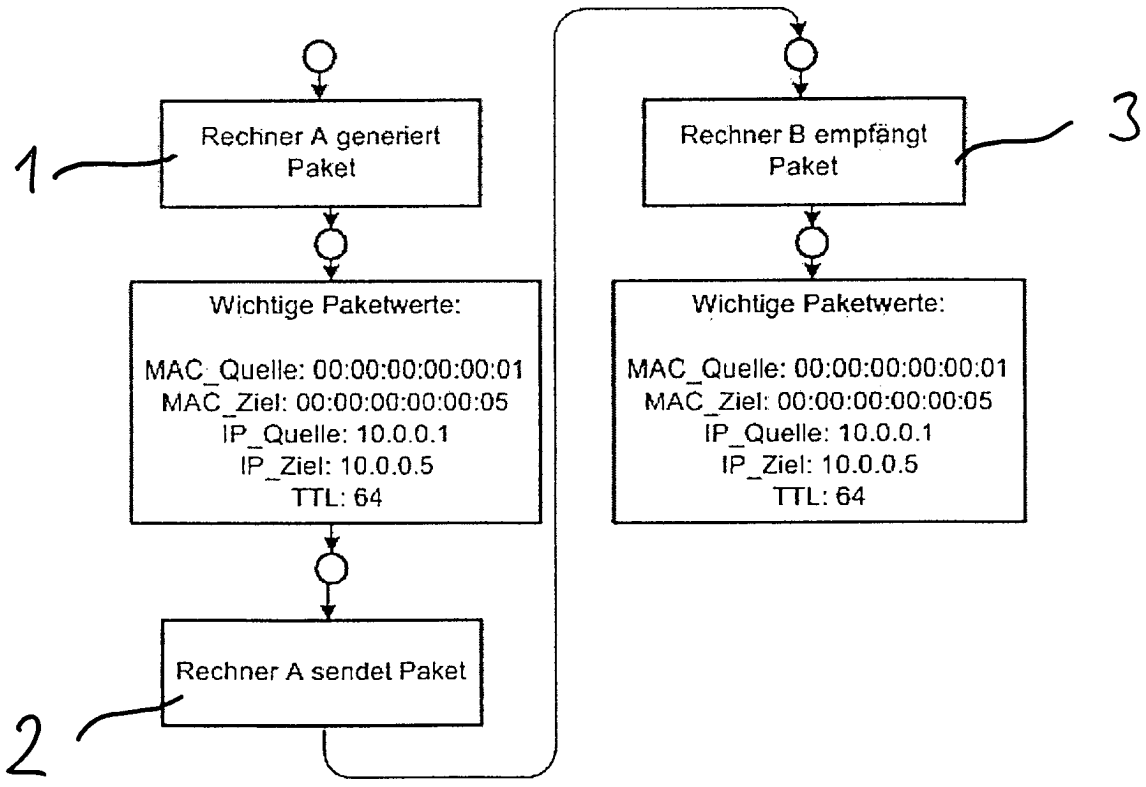

1
Rechner A generiert Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64
2
Rechner A sendet Paket
3
Rechner B empfängt Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64

Fig. 4

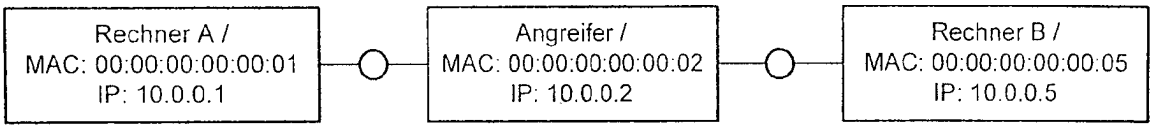

Rechner A /
MAC: 00:00:00:00:00:01
IP: 10.0.0.1
Angreifer /
MAC: 00:00:00:00:00:02
IP: 10.0.0.2
Rechner B /
MAC: 00:00:00:00:00:05
IP: 10.0.0.5

Fig. 5

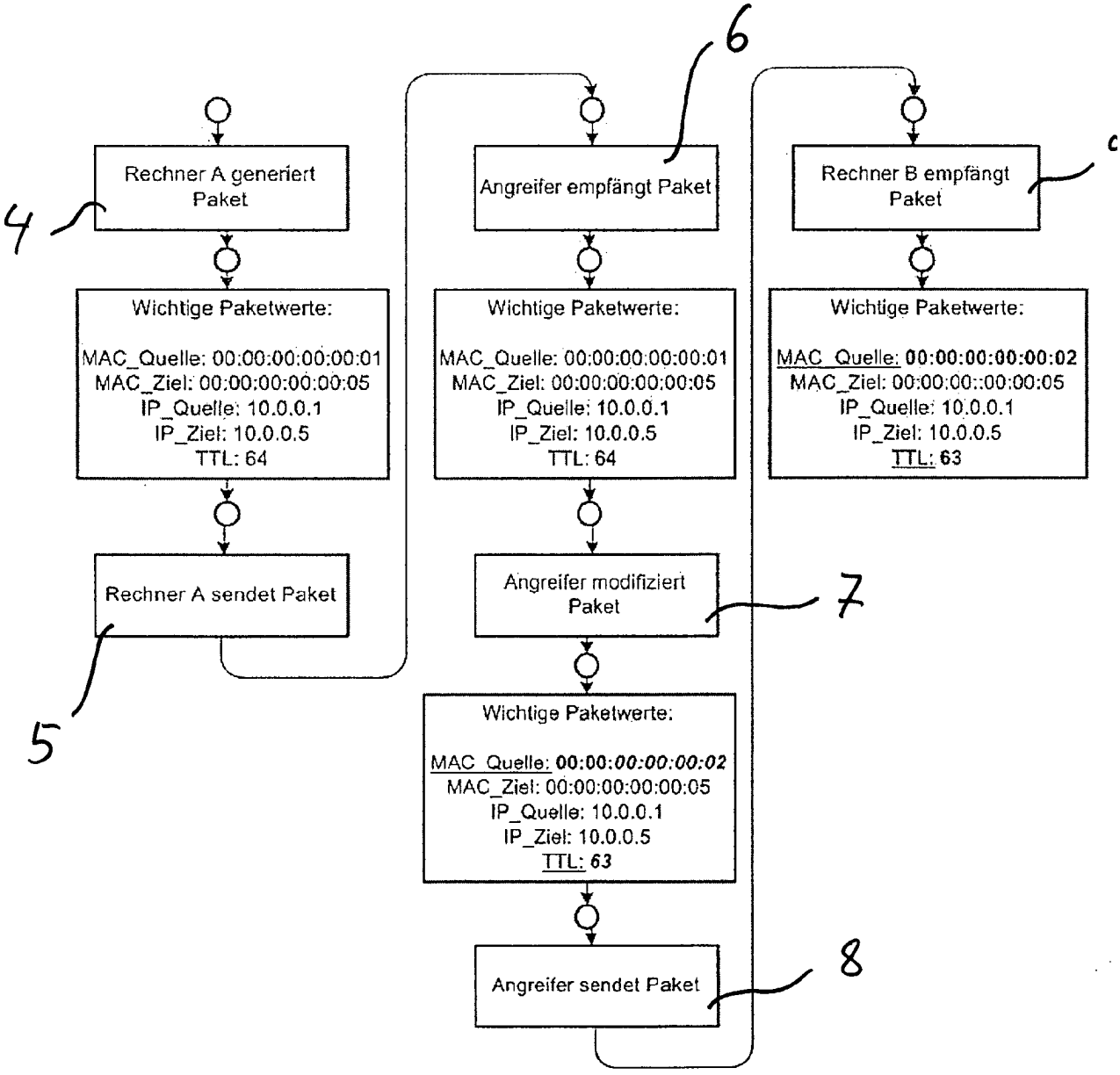

4
Rechner A generiert Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64
Rechner A sendet Paket
5
6
Angreifer empfängt Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64
Angreifer modifiziert Paket
7
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:02
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 63
Angreifer sendet Paket
8
Rechner B empfängt Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:02
MAC_Ziel: 00:00:00::00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 63

Fig. 6

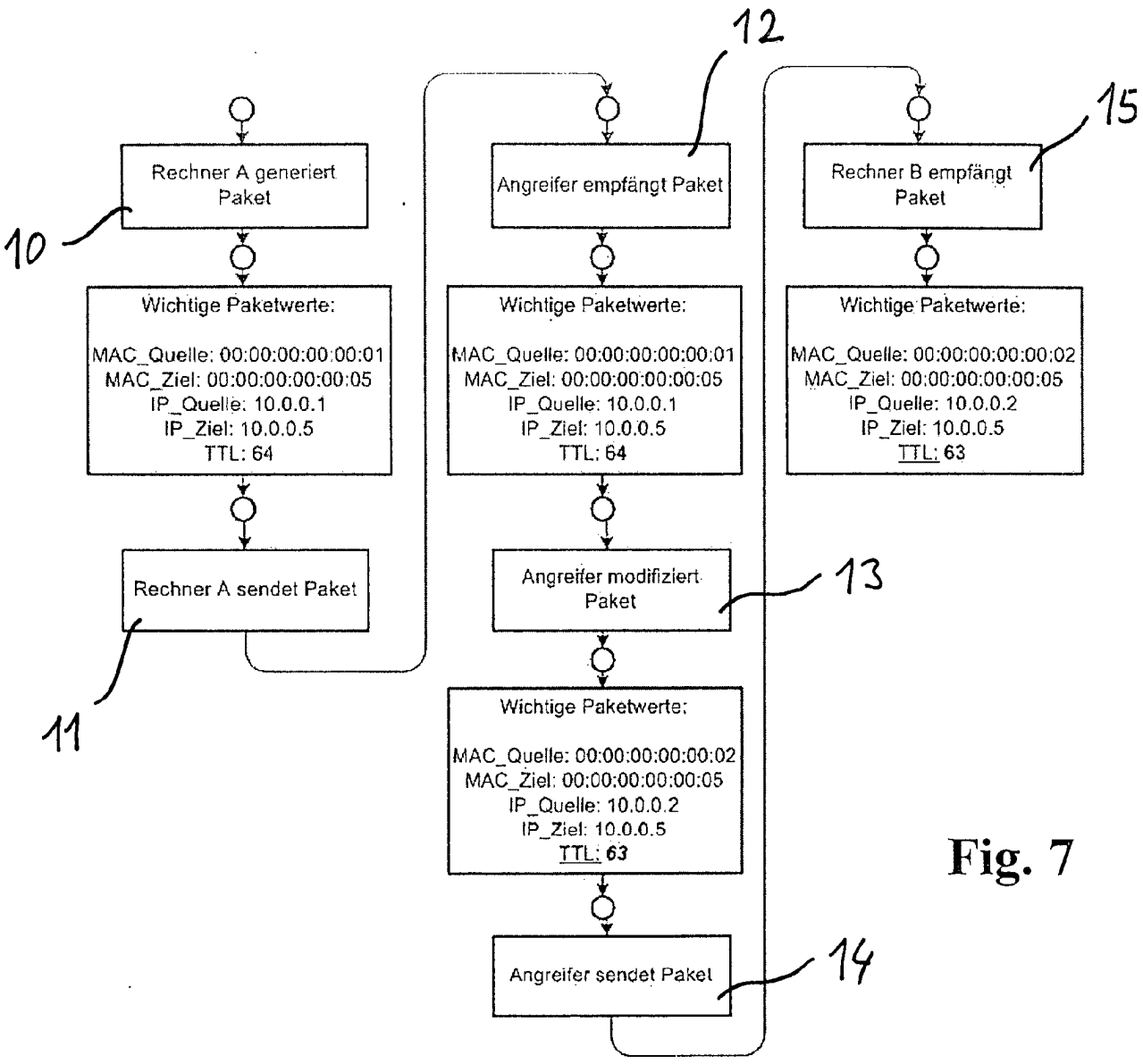

Rechner A generiert Paket
10
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64
Rechner A sendet Paket
11
12
Angreifer empfängt Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:01
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.1
IP_Ziel: 10.0.0.5
TTL: 64
Angreifer modifiziert Paket
13
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:02
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.2
IP_Ziel: 10.0.0.5
TTL: 63
Angreifer sendet Paket
14
15
Rechner B empfängt Paket
Wichtige Paketwerte:
MAC_Quelle: 00:00:00:00:00:02
MAC_Ziel: 00:00:00:00:00:05
IP_Quelle: 10.0.0.2
IP_Ziel: 10.0.0.5
TTL: 63

Fig. 7

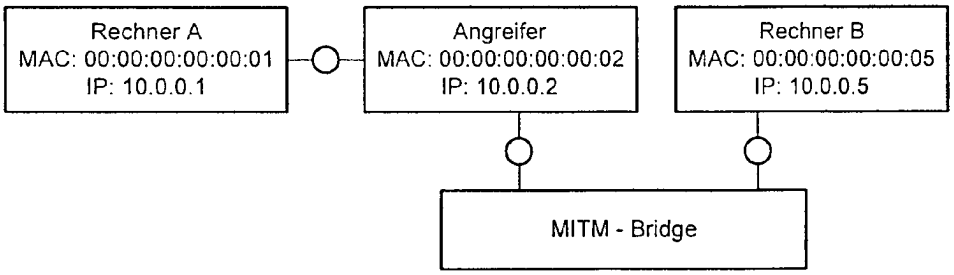

Rechner A
MAC: 00:00:00:00:00:01
IP: 10.0.0.1
Angreifer
MAC: 00:00:00:00:00:02
IP: 10.0.0.2
Rechner B
MAC: 00:00:00:00:00:05
IP: 10.0.0.5
MITM - Bridge

Fig. 8

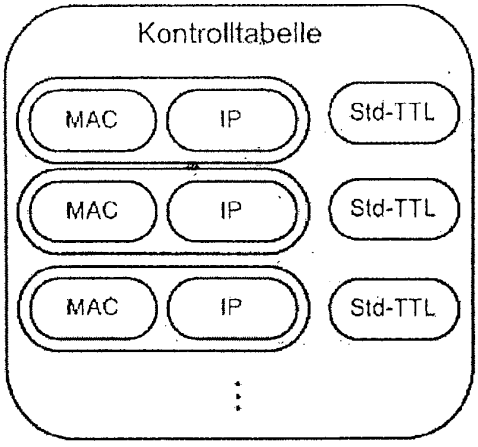

Kontrolltabelle
MAC
IP
Std-TTL
MAC
IP
Std-TTL
MAC
IP
Std-TTL

Fig. 9

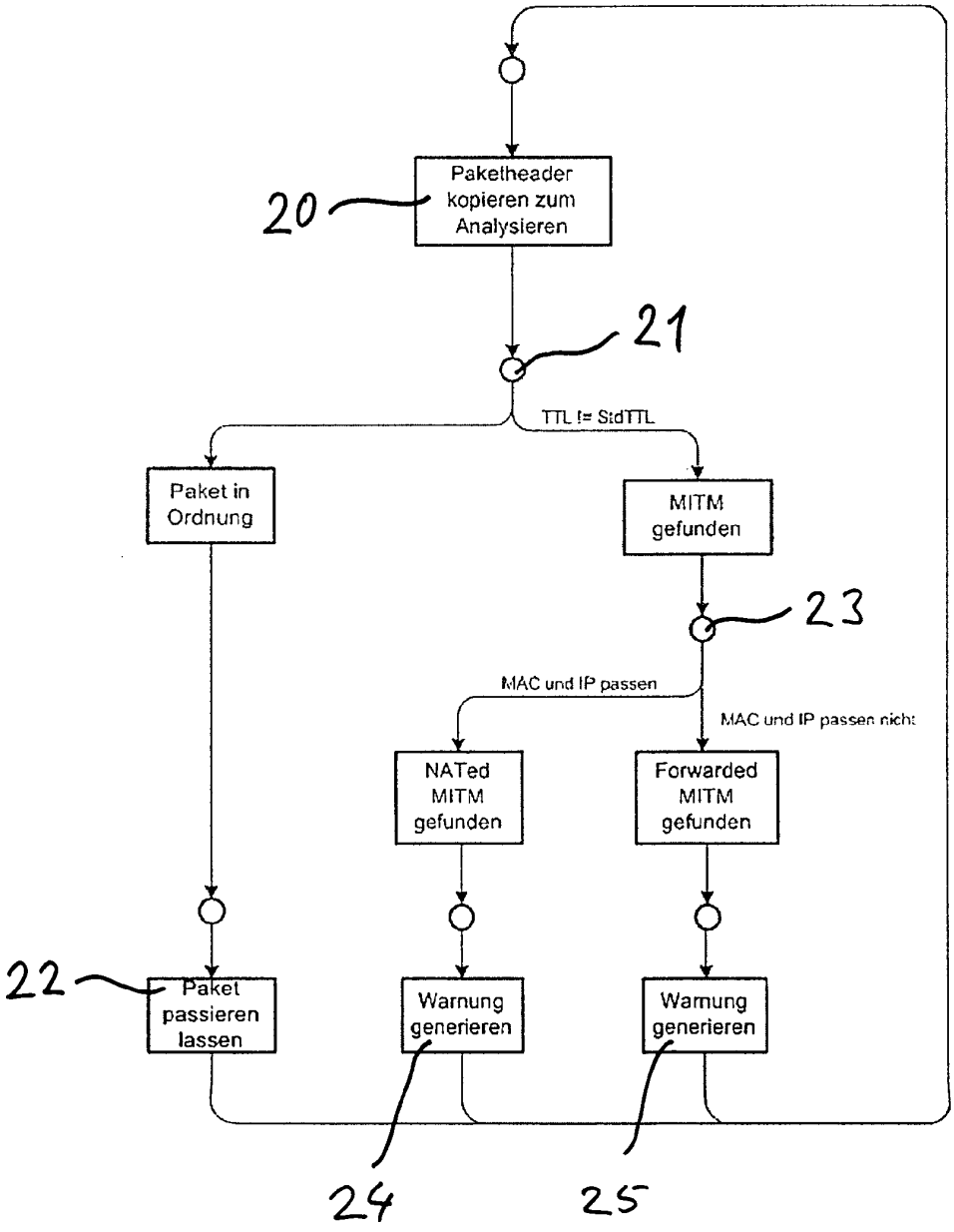

Paketheader kopieren zum Analysieren
20
21
TTL != StdTTL
Paket in Ordnung
MITM gefunden
23
MAC und IP passen
MAC und IP passen nicht
NATed MITM gefunden
Forwarded MITM gefunden
22
Paket passieren lassen
Warnung generieren
Warnung generieren
24
25

Fig. 10

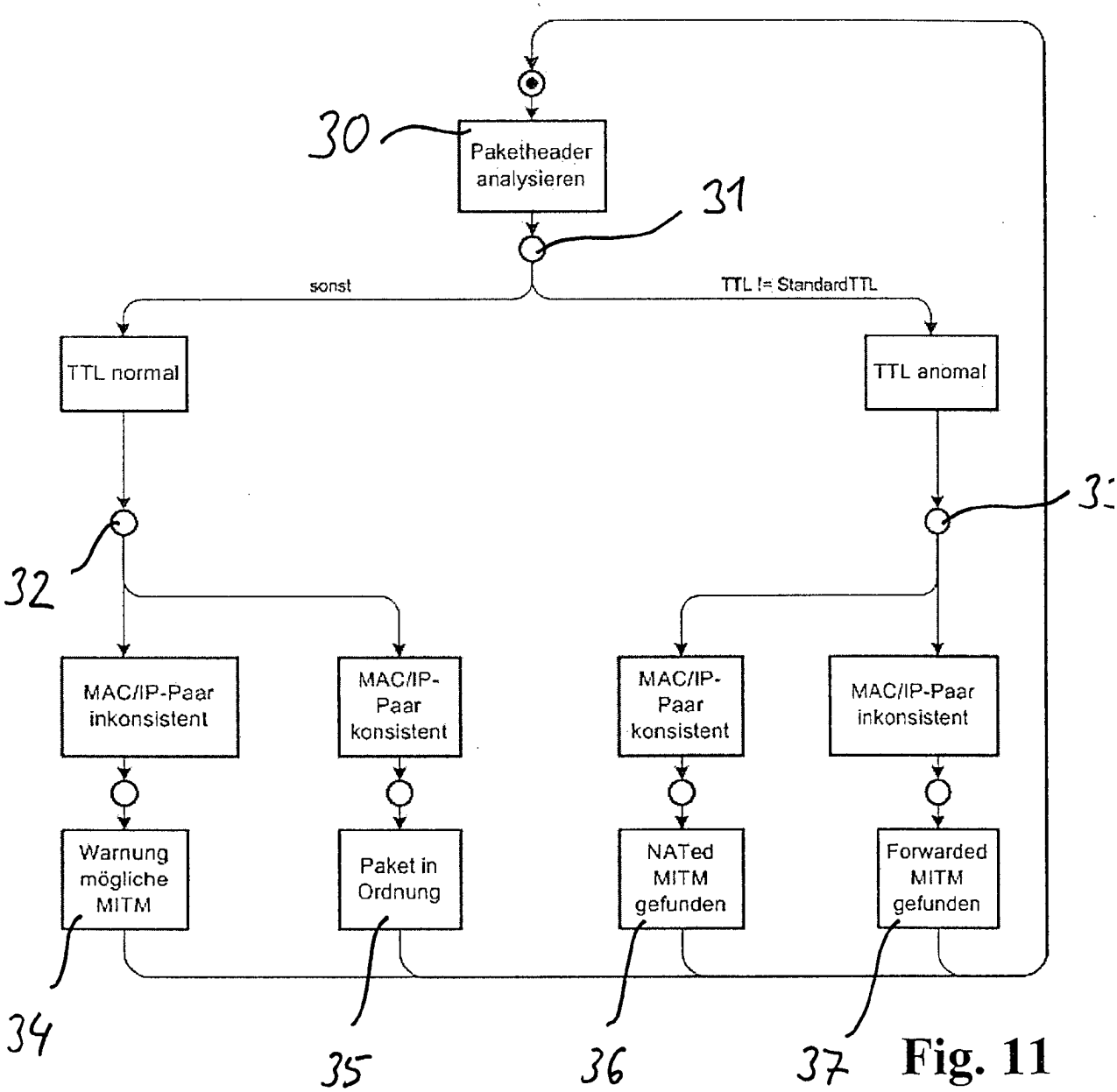

30
Paketheader analysieren
31
sonst
TTL != StandardTTL
TTL normal
TTL anomal
32
MAC/IP-Paar inkonsistent
MAC/IP-Paar konsistent
MAC/IP-Paar konsistent
MAC/IP-Paar inkonsistent
Warnung mögliche MITM
Paket in Ordnung
NATed MITM gefunden
Forwarded MITM gefunden
34
35
36
37

Fig. 11