(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4059388号
(P4059388)
(45)発行日　平成20年3月12日(2008.3.12)　(24)登録日　平成19年12月28日(2007.12.28)

(51)Int.Cl.　F I
H04L 29/04 (2006.01)　H04L 13/00　303B

請求項の数 7　(全 22 頁)

(21)出願番号　特願2002-221254(P2002-221254)
(22)出願日　平成14年7月30日(2002.7.30)
(65)公開番号　特開2003-60727(P2003-60727A)
(43)公開日　平成15年2月28日(2003.2.28)
審査請求日　平成17年6月14日(2005.6.14)
(31)優先権主張番号　09/919,297
(32)優先日　平成13年7月31日(2001.7.31)
(33)優先権主張国　米国(US)

(73)特許権者　399117121
アジレント・テクノロジーズ・インク
ＡＧＩＬＥＮＴ　ＴＥＣＨＮＯＬＯＧＩＥＳ，　ＩＮＣ．
アメリカ合衆国カリフォルニア州サンタクララ　スティーブンス・クリーク・ブルーバード　５３０１
(74)代理人　100099623
弁理士　奥山　尚一
(72)発明者　ジェリー・デイヴィッド・モリス
アメリカ合衆国８０９０４コロラド州コロラド・スプリングス、クラウン・リッジ・ドライブ　８１８

最終頁に続く

(54)【発明の名称】プロトコルデータ単位内のプロトコルパターンの識別装置及び方法

(57)【特許請求の範囲】
【請求項１】
プロトコル識別装置により実行可能な指令からなるコンピュータプログラムを具現化して、各層においてデータをプロトコルデータ単位内にカプセル化するのに用いたコンピュータネットワークプロトコルを識別する方法ステップを実行する、プロトコル識別装置によって読み取り可能な記憶媒体であって、ここで、ステージとは、前記カプセル化するのに用いた前記コンピュータネットワークプロトコルが識別される層に対応するものであり、
前記方法ステップは、
データと複数のカプセル化プロトコルパターンを含むプロトコルデータ単位を受け取るステップと、
予め定めた検索パターンのグループのうち少なくとも１つについてグループ指標を割り当てるステップであって、前記グループは少なくとも１つの予め選択された検索パターンを含む少なくとも１つのサブセットを含み、前記予め選択された検索パターンはデータをカプセル化するのに用いる予め選択された少なくとも１つのネットワークプロトコルを識別するためのものである、ステップと、
前記グループ指標を初期化し、少なくとも１つの前記サブセットがプロトコルデータ単位内の予想された位置に存在することを指定するステップと、
前記プロトコルデータ単位を検索する少なくとも１つのステージが残っている間に、
残りのステージのうちの１つを選択することと、

前記プロトコルデータ単位を検索するための前記選択されたステージに少なくとも１つの検索パターンが残っている間に、
残りの検索パターンのうちの１つを選択することと、
選択された検索パターンを捜して前記プロトコルデータ単位を検索することと
を繰り返し実行することと、
前記選択されたステージについてのグループの各サブセットに関連する全ての検索パターンがプロトコルデータ単位の予想された位置に存在しない場合、そのグループの全サブセットがプロトコルデータ単位に存在しないことを指定するように、前記グループ指標を設定することと
を繰り返し実行するステップと
を含むものである、記憶媒体。

【請求項２】
前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップに続いて、前記方法ステップは、
少なくとも１つのステージが残っている間の繰り返しループの後に、
プロトコルデータ単位内の予想された位置に少なくとも１つのサブセットが存在する場合、そのプロトコルデータ単位をバッファに配置するステップをさらに含む、
請求項１に記載の記憶媒体。

【請求項３】
前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップは、
プロトコルデータ単位を検索する選択されたステージの検索パターンの少なくとも一部が残っている間に、
選択された検索パターンの残っている未検索部分のうちの１つを選択するステップと、
選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
を繰り返し実行することをさらに含む、請求項１に記載の記憶媒体。

【請求項４】
前記方法ステップは、
前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが前記プロトコルデータ単位内の選択部分を見つけられなかった場合、
プロトコルデータ単位を検索する前記選択されたステージの検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップと、
プロトコルデータ単位を検索する前記選択されたステージの少なくとも１つの検索パターンが残っている間の繰り返しループを抜け出すステップと、
をさらに含む、請求項３に記載の記憶媒体。

【請求項５】
前記残っている検索パターンの１つを選択するステップに続いて、前記方法ステップは、
プロトコルデータ単位を検索する前記選択されたステージの少なくとも１つの他の検索パターンが残っている場合、
前記他の残っている検索パターンのうち少なくとも１つを選択するステップと、
前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンを捜してプロトコルデータ単位を検索するステップと、
をさらに含む、請求項１に記載の記憶媒体。

【請求項６】
前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンを捜してプロトコルデータ単位を検索するステップは、

プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部と、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部とが残っている間に、

前記選択された検索パターンの残っている未検索部分の１つを選択するステップと、

前記他の選択された検索パターンの残っている未検索部分の１つを選択するステップと、

選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、

前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、

をさらに含み、

あるいは、プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部が残っている間に、

前記選択された検索パターンの残っている未検索部分の１つを選択するステップと、

選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、

を繰り返し実行することをさらに含み、

あるいは、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部が残っている間に、

前記他の選択された検索パターンの残っている未検索部分の１つを選択するステップと、

前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、

を繰り返し実行することをさらに含む、

請求項５に記載の記憶媒体。

【請求項７】

前記方法ステップは、

前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に選択された検索パターンの選択部分を見つけられなかった場合、及び、前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索する並行ステップが、プロトコルデータ単位内に他の選択された検索パターンの選択部分を見つけられなかった場合に、

プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部と、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部とが残っている間の繰り返しループを抜け出すステップをさらに含み、

あるいは、選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に選択された検索パターンの選択部分を見つけられなかった場合、

プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップをさらに含み、

あるいは、他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に他の選択された検索パターンの選択部分を見つけられなかった場合、

プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップをさらに含む、

請求項６に記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】
本発明は、コンピュータネットワークシステムにおいて、一般にプロトコルデータ単位（ＰＤＵ）と呼ばれるデータのパケットやフレームをそれらのカプセル化に用いるプロトコルの点から識別し、さらにそのように識別されたデータパケットを選択しまたはフィルタリングすることに関する。
【０００２】
【従来の技術】
最新のコンピュータネットワークは、相互接続されたコンピュータの集合体からなる。このようなネットワークの主要機能は、所属コンピュータ間の情報交換を可能にすることである。一般に、所属コンピュータは、他のコンピュータがネットワーク経由で情報伝送を試みる時点に関して制御することなく、自律的に動作するので、一般にデータは多数のより小さな塊に分割され、そのデータの塊がパケットまたはフレームの中に入れられて独立して伝送される。この実施により、ネットワークへのアクセスがより均等になる上に、ネットワークに接続された様々なコンピュータのパケット間で衝突が発生した場合にパケットを再送する機会が得られる。所与のパケットは、割り当てられたデータの部分とパケットのフォーマットを規定する情報の他、パケット番号やパケット送受信者のアドレスといった他の情報も含む。データパケットのフォーマットは、予め規定されたプロトコルによって特定される。データパケットのフォーマット化は、ネットワークが階層構造をなしているという事実により複雑なものとなっている。一般に、データパケットはそれぞれ固有のプロトコルを持つネットワーク層により次々と連続的にカプセル化されていく。作成されたデータパケットは、多くの場合プロトコルデータ単位（ＰＤＵ）と呼ばれる。さらに複雑なことに、多数の異なるプロトコルがネットワークの様々な層で共通して使用されていることがある。特定のカプセル化プロトコルが使用されたことを示す任意の所与のプロトコルデータ単位に付加されるビットパターンが予め指定された長さの組のから選択された長さを有する一方で、異なるプロトコルが別の予め指定された長さの組から選択された長さを有する場合もある。さらに、未知のプロトコルを用いる無関係なコンピュータのグループが同じネットワークに接続されて、同じネットワークを使用することもある。
【０００３】
ネットワーク環境は、複雑で動的である。従って、ネットワーク管理における非常に重要な作業は、搬送する通信量の分析である。この目的のために、プロトコル解析器が用いられる。プロトコル解析器は一般に、様々な予め選択されたプロトコルによってカプセル化されたプロトコルデータ単位の識別を試みる。このような識別の従来の方法は、対象プロトコルの予め定めた組み合わせを識別するフィルタやパターン比較器の使用に頼ってきた。プロトコルの任意の所与の組み合わせは、パケットをカプセル化するのに使用したプロトコルのサブパターンを含むビットパターンを形成し、これらのサブパターンはそれぞれプロトコルデータ単位内の特定の固定オフセットで開始する。予測されたパターンの組合せに一致するこれらのプロトコルデータ単位のみが、任意の所与のフィルタによる照合の基準を満たすものとして識別される。このようなフィルタは、「フラットフィルタ」と呼ばれる。この技法の顕著な特徴は、対象プロトコルの組み合わせ毎に１つのフィルタが必要であることである。
【０００４】
従って、この手法には、多数のフィルタ、実際には多数のビットパターン比較器を使用する必要があるという不利がある。例えば、ユーザがプロトコルｘＧＣＰ上の音声トラフィックを含むプロトコルデータ単位を探しているとすると、現行１３個のフラットフィルタが必要となる。また、３つの異なるローカルエリアネットワーク（ＬＡＮ）カプセル化のうちのどれが用いられているかをユーザが知らない場合は、１３個のフィルタを３組、つまり合計計３９個のフラットフィルタが必要となる。さらに、６つの異なる広域ネットワーク（ＷＡＮ）カプセル化のうちのどれがＬＡＮトラフィックの搬送に用いられているかをユーザが知らない場合は、３９個のフィルタを６組、つまり合計２３４個のフィルタ用が必要となる。このような状況では、ハードウェア資源が非常に高価かつ複雑になる。こ

のように、ハードウェア資源を設けることは非実用的である。

【０００５】

また、一般のネットワーク状況では、文字通り数百の異なるノード間を流れるデータが存在し得るが、ユーザがデータを捕捉する対象とするのはそのうち２つからだけである。最新ネットワークの速度と典型的な最新ネットワーク解析器の限られたメモリ空間のために、プロトコルデータ単位の捕捉に割り当てられるバッファ空間はすぐにオーバーランしてしまうおそれがある。捕捉される大多数のプロトコルデータ単位は、ユーザが対象としないノードからのものであることもあり得る。一例として、対象となる２つのノードのＩＰ（インターネットプロトコル）アドレスをユーザが知っていて、これらの２つのノード間のデータのみを捕捉したいとき、ユーザがネットワークの詳しい知識をもたない場合は、上記の多数のフラットフィルタを自在に操らない限り、プロトコルデータ単位のＩＰアドレスを識別することはできない。

【０００６】

【発明が解決しようとする課題】

プロトコルデータ単位をカプセル化するのに用いる複数のプロトコルの組み合わせを識別するより優れた技術に対する要望が存在する。特に、現行システムが行なっているような多数のフィルタを必要としない、関連パケットのフィルタリングを用いたこのような識別が可能なシステムに対する要望が存在する。

【０００７】

【課題を解決するための手段】

本発明は、コンピュータネットワークシステムにおける可変長、多層カプセル化プロトコルデータパケットの識別と、関連するフィルタリングについての新規な方法に関する。このような識別及び関連するフィルタリングのための従来の方策は、対象とするプロトコルの所定の組み合わせをそれぞれ識別する多数のフラットフィルタを用いることに頼ってきた。多くの状況では、必要となるフラットフィルタが多数となるため、ハードウェア資源が非常に高価となり、従ってハードウェア資源を設けることは非実用的である。

【０００８】

代表的な実施形態において、本発明は、コンピュータネットワークプロトコルデータ単位を段階的に識別してフィルタリングするプロトコル識別装置を使用する技術を開示する。第１のステージにおいて、本装置は、潜在的なプロトコルビットパターンの組とプロトコルデータ単位のビットを照合して、カプセル化の第１の層に使用されたプロトコルを識別する。次にプロトコル識別装置は、プロトコルビットパターンの第２の組と同様の照合を行うか、先のカプセル化プロトコル内へ符号化された情報によるか、先の照合に基づいて装置内に符号化された最良の推定または装置内に符号化されたユーザの推定によるかして、選択する次のカプセル化層の識別を試みる。このプロセスは、ユーザが対象とする全てのカプセル化層が識別されるまで継続する。このようなパターンは、それぞれ異なる長さとすることができる。しかし、一旦任意の所与のプロトコルカプセル化層が識別されると、本装置は、次のプロトコルパターンの検索を開始するためにプロトコルデータ単位内にどの程度分け入ってインデックス付けすべきかを知る。このプロセスは、所与の実装の制約内であれば、必要なだけ何度でも繰り返すことができる。

【０００９】

任意の所与のプロトコル層のパターンの数を簡単に並列検索し比較できるようにするために、テーブル参照方式が使用される。プロトコル識別装置は、プロトコルデータ単位内のどの箇所で最後に照合したプロトコルパターンの終端が生じたかを知っているので、次のパターン照合の試みを開始する箇所も知っている。

【００１０】

開示する技法は、ステージの概念を利用する。プロトコル識別装置は、各ステージ内で、プロトコルカプセル化の１つの層について、プロトコルデータ単位ビットと予め定義されたパターンビットとの間のパターンの一致を発見するよう試みる。一旦発見すると、装置は自らリセットし、次のカプセル化層についての新規の検索を開始する。

【００１１】
代表的な実施形態では、開示する技法はプロトコルデータ単位を段階的に検索することと考えることができる。各ステージは、典型的に予め割り当てられた番号を有する。プロトコルデータ単位の検索は、例えばステージ番号０において開始され、そのステージによる検索が完了すると、現在のステージ検索結果に基づいて新しいステージが選択される。このプロセスは、プロトコルデータ単位の終端に達するまで、またはそれ以上のプロトコルデータ単位の検索が不要であると制止されるまで継続される。
【００１２】
プロトコルデータ単位のバイトは、例えばバイト０から始まって検索される。このステージは、ステージを終了させるパターンが発見されるまでプロトコルデータ単位のバイトを消費するものと考えることができる。次のステージは、最後のステージが終了したバイトを消費することから開始する。選択的に、パターン内で照合する必要のないバイトをスキップすることで、この処理に対して性能の向上を図ることができる。スキップすべきバイトはテーブル内に予めプログラムされ、そのテーブルがシステムによって使用されて不要なバイトをスキップする。
【００１３】
代表的な実施形態では、任意の所与のステージにおけるプロトコルパターン検索に用いられる方法及び装置は、連続するステージ検索のそれぞれのために繰り返し使用される。予めプログラムされた「パターン参照テーブル」を使用して、現在のステージについてプロトコルデータ単位の特定部分に特定のカプセル化が存在するか否かが判定される。パターン参照テーブルの一部は、現在のステージ番号と検索中のプロトコルデータ単位バイト番号について予めプログラムされおり、インデックス付けがなされる。代表例では、「パターン参照」テーブルのこの部分は２５６個のエントリを有しており、その１つ１つがプロトコルデータ単位の現在のバイトのとり得る値を有する。プロトコルデータ単位の現在のバイトの実際の値に対応するエントリは、テーブルから読み込まれる。パターン参照テーブルから読み込まれた値は、ＡＮＤを取られステージ蓄積器へ蓄積される。この蓄積器は通常ステージの始まりで全て１に初期化される。
【００１４】
このステージ蓄積器の値の各ビットは、それぞれ割り当てられたパターン番号を有する。そのステージ蓄積器ビットがセットされ、そのステージがプロトコルデータ単位内に十分分け入って検索してパターン全体に一致した場合、１つのパターンが「エントリリスト」内の予めプログラムされた値から決定されたものとして発見されたとみなされ、これにより「ステージパターン発見ビット」がセットされる。代表例では、エントリリストは、例えば次のスキップ値とこのステージについての最後のパターン比較といった情報を提供する１つのエントリをパターンの比較毎に有している。新しいステージへ移行させるよう指定されたパターンが発見された場合、現在のステージは終了し、発見されない場合、プロトコルデータ単位の終端へは達してしないものと仮定して、次のパターン参照テーブルエントリが読み取られる。
【００１５】
現在のステージについてのパターンに関する予めプログラムされた情報に基づいて、どのプロトコルが発見され、次にどのステージ番号へ進み、「ステージグループ結果」の形成に当たり使用されるどのパターン番号が発見されたか、さらに時にはたった今発見されたカプセル化の後にどのカプセル化が続くのかに関する情報を出力することができる。ステージグループ結果は、完了したステージについてのパターン照合の結果である。一般に、グループ結果は、対応するビット位置に１が置かれるその予め選択された検索パターンのグループについて一致が見つからない限り、各ステージについて予め選択された検索パターングループを表わすそれぞれのビット位置に０を持つビットパターンである。グループ結果は、プロトコルデータ単位が予め選択されたプロトコルのグループに一致するか否かを判定するために使用することができる。
【００１６】

各ステージの検索が終わると、そのステージについてどのパターンが発見されたかを示すビットが「ステージグループ結果」にマッピングされる。このマッピングは、本明細書では「クリーク（clique）マップ」と呼ばれる多数の予めプログラムされたテーブルを使用することで達成される。各クリークマップは、現在のステージ番号とクリークマップに割り当てられたステージパターン発見ビットのビットに基づいてインデックス付けされる。選択的に、必要とされる「ステージグループ結果ビット」の数がクリークマップの幅よりも大きいときは、クリークマップ内へのインデックス付けはさらに「時間スライス番号」に基づかせることもできる。

【００１７】

各クリークマップから得られる値はＯＲをとられ、「ステージグループ結果値」を形成する。このステージグループ結果からの幾つかのビットは、任意の数のステージ出力結果を生成するために選択的に使用することができるが、他の方法もステージ出力の生成に使用することができる。また、残りのステージグループ結果ビットは、「ステージグループフィルタ結果」の形成に使用される。ステージグループフィルタ結果はＡＮＤを取られグループ蓄積器に蓄積される。この蓄積器はプロトコルデータ単位の検索の開始時に全て１に初期化される。このグループ蓄積器の値の各ビットは、割り当てられた「グループフィルタ番号」を有する。

【００１８】

グループフィルタは条件を満たしたステージの予め選択されたセットとして指定され、各指定されたステージ内でそのステージ用に指定されたパターンのうちの１つだけが条件を満たすステージについて発見される。プロトコルデータ単位の検索の完了時に、そのグループ蓄積器ビットがセットされかつ適当なステージがプロトコルデータ単位を検索した場合に、グループフィルタが見つかったとみなされる。従来のフィルタ設計を用いる場合と同じく、グループフィルタの発見の結果として、カウント、プロトコルデータ単位の保存、プロトコルデータ単位の廃棄、データ捕捉の開始または停止などの１つまたは複数の動作を他の動作と同様に行なうことができる。

【００１９】

本明細書に開示される技術は、どの下位層プロトコルが使用されているかを一切知ることなく、上位層のプロトコルにおいてユーザが何かを捜すことができる能力をもたらすものである。また、所望のカプセル化パターンに関する情報を本装置に知らせることによって、本装置は実行時にプロトコルデータ単位におけるカプセル化を識別することができ、これによって、追加のソフトウェアルーチンがその後に各パケットにおけるカプセル化の識別にかかる時間を節約する。本装置をハードウェア及びソフトウェアの両方で実装することで、プロトコルデータ単位を高速に識別することができる。

【００２０】

一般のネットワーク状況では、文字通り数百の異なるノード間を流れるデータが存在し得るが、ユーザがデータを捕捉する対象とするのはそのうち２つからだけである。最新ネットワークの速度と典型的な最新ネットワーク解析器の限られたメモリ空間のために、プロトコルデータ単位の捕捉に割り当てられるバッファ空間はすぐにオーバーランしてしまうおそれがある。従来のシステムでは、捕捉される大多数のプロトコルデータ単位は、ユーザが対象としないノードからのものであることもあり得る。一例として、対象となる２つのノードのＩＰ（インターネットプロトコル）アドレスをユーザが知っており、これらの２つのノード間のデータのみを捕捉したいとき、ユーザがネットワークの詳しい知識をもたない場合は、上記の多数のフラットフィルタを自在に操らない限り、プロトコルデータ単位のＩＰアドレスを識別することはできない。しかし、本発明による装置の様々なステージでの識別の能力をもってすれば、プロトコルの識別に必要なものを越える僅かな追加の努力だけで、対象とするこれらのプロトコルデータ単位のフィルタリングが可能となる。

【００２１】

従来技術に対する本発明の実施形態の主要な利点は、プロトコルデータ単位をパケットプ

ロトコルパターンと照合するのに必要となる多数のパターン比較器を大きく低減することである。この低減は、ステージという概念の利用によってもたらされる。さらなる利点は、使用されている低位層のプロトコルについての知識を持つことなく、高位層のプロトコルにおける特定のパターンを検索する能力である。また、本装置をハードウェア及びソフトウェアの両方で実装することで、プロトコルデータ単位を高速に識別することができる。他の利点は、特定のプロトコルデータ単位内にどのようなカプセル化が存在するかについての情報を提供し、従って後に各パケットを処理するときのソフトウェアルーチン所要時間を節約する能力である。最後に、所望のカプセル化パターンに関する情報をプロトコル識別装置に知らせることにより、プロトコル識別装置は、実行時にプロトコルデータ単位をフィルタリングすることができ、これにより、不必要なパケットを後で処理するために追加のソフトウェアルーチンが費やす時間を節約するという利点が得られ、また対象としないプロトコルデータ単位を廃棄することで、貴重な捕捉バッファ空間が得られる。

【００２２】

【発明の実施の形態】

説明のために図中に示したように、本発明はコンピュータネットワークシステム内での可変長の多層カプセル化プロトコルデータパケットの識別と、関連するフィルタリングのための新規な方法に関するものである。このような識別及び関連するフィルタリングに対する従前の解決策は、対象プロトコルの所定の組み合わせをそれぞれ識別する多数のフラットフィルタの使用に頼っていた。多くの状況では、必要となるフラットフィルタの数が大きいために、ハードウェア資源が非常に高価となり、従ってそれらを非実用的なものにしている。

【００２３】

１．緒言

代表的な実施形態では、本発明は、コンピュータネットワークプロトコルデータ単位を段階的に識別してフィルタリングするプロトコル識別装置を使用する技術を開示する。第１のステージにおいて、本装置は、潜在的なプロトコルビットパターンの組とプロトコルデータ単位のビットを照合して、カプセル化の第１の層に使用されたプロトコルを識別する。次に本装置は、プロトコルビットパターンの第２の組と同様の照合を行うか、先のカプセル化プロトコル内へ符号化された情報によるか、先の照合に基づいて装置内に符号化された最良の推定または装置内に符号化されたユーザの推定によるかして、選択する次のカプセル化層の識別を試みる。このプロセスは、ユーザが対象とする全てのカプセル化層が識別されるまで継続する。このようなパターンは、それぞれ異なる長さとすることができる。しかし、一旦任意の所与のプロトコルカプセル化層が識別されると、本装置は、次のプロトコルパターンの検索を開始するためにプロトコルデータ単位内にどの程度分け入ってインデックス付けすべきかを知る。このプロセスは、所与の実装の制約内であれば、必要なだけ何度でも繰り返すことができる。

【００２４】

任意の所与のプロトコル層のパターンの数を簡単に並列検索し比較できるようにするために、テーブル参照方式が使用される。本装置は、プロトコルデータ単位内のどの箇所で最後に照合したプロトコルパターンの終端が生じたかを知っているので、次のパターン照合の試みを開始する箇所も知っている。

【００２５】

開示する技法は、ステージの概念を利用する。本装置は、各ステージ内で、プロトコルカプセル化の１つの層について、プロトコルデータ単位ビットと予め定義されたパターンビットとの間のパターンの一致を発見するよう試みる。一旦発見すると、装置は自らリセットし、次のカプセル化層についての新規の検索を開始する。

【００２６】

代表的な実施形態では、開示する技法はプロトコルデータ単位を段階的に検索することと考えることができる。各ステージは、一般に予め割り当てられた番号を有する。プロトコルデータ単位の検索は、例えばステージ番号０において開始され、そのステージによる検

索が完了すると、現在のステージ検索結果に基づいて新しいステージが選択される。このプロセスは、プロトコルデータ単位の終端に達するまで、またはそれ以上のプロトコルデータ単位の検索が不要であると制止されるまで継続される。

【００２７】

プロトコルデータ単位のバイトは、例えばバイト０から始まって検索される。このステージは、ステージを終了させるパターンが発見されるまでプロトコルデータ単位のバイトを消費するものと考えることができる。次のステージは、最後のステージが終了したバイトを消費することから開始する。選択的に、パターン内で照合する必要のないバイトをスキップすることで、この処理に対して性能の向上を図ることができる。スキップすべきバイトはテーブル内に予めプログラムされ、そのテーブルがシステムによって使用されて不要なバイトをスキップする。

【００２８】

代表的な実施形態では、任意の所与のステージにおけるプロトコルパターン検索に用いられる方法及び装置は、連続するステージ検索のそれぞれのために繰り返し使用される。予めプログラムされた「パターン参照テーブル」を使用して、現在のステージについてプロトコルデータ単位の特定部分に特定のカプセル化が存在するか否かが判定される。パターン参照テーブルの一部は、現在のステージ番号と検索中のプロトコルデータ単位バイト番号について予めプログラムされおり、インデックス付けがなされる。代表例では、「パターン参照」テーブルのこの部分は２５６個のエントリを有しており、その１つ１つがプロトコルデータ単位の現在のバイトのとり得る値を有する。プロトコルデータ単位の現在のバイトの実際の値に対応するエントリは、テーブルから読み込まれる。パターン参照テーブルから読み込まれた値は、ＡＮＤを取られステージ蓄積器へ蓄積される。この蓄積器は通常ステージの始まりで全て１に初期化される。

【００２９】

このステージ蓄積器の値の各ビットは、それぞれ割り当てられたパターン番号を有する。そのステージ蓄積器ビットがセットされ、そのステージがプロトコルデータ単位内に十分分け入って検索してパターン全体に一致した場合、１つのパターンが「エントリリスト」内の予めプログラムされた値から決定されたものとして発見されたとみなされ、これにより「ステージパターン発見ビット」がセットされる。代表例では、エントリリストは、例えば次のスキップ値とこのステージについての最後のパターン比較といった情報を提供する１つのエントリをパターンの比較毎に有している。新しいステージへ移行させるよう指定されたパターンが発見された場合、現在のステージは終了し、発見されない場合、プロトコルデータ単位の終端へは達してしないものと仮定して、次のパターン参照テーブルエントリが読み取られる。

【００３０】

現在のステージについてのパターンに関する予めプログラムされた情報に基づいて、どのプロトコルが発見され、次にどのステージ番号へ進み、「ステージグループ結果」の形成に当たり使用されるどのパターン番号が発見されたか、さらに時にはたった今発見されたカプセル化の後にどのカプセル化が続くのかに関する情報を出力することができる。ステージグループ結果は、完了したステージについてのパターン照合の結果である。一般に、グループ結果は、対応するビット位置に１が置かれるその予め選択された検索パターンのグループについて一致が見つからない限り、各ステージについて予め選択された検索パターングループを表わすそれぞれのビット位置に０を持つビットパターンである。グループ結果は、プロトコルデータ単位が予め選択されたプロトコルのグループに一致するか否かを判定するために使用することができる。

【００３１】

各ステージの検索が終わると、そのステージについてどのパターンが発見されたかを示すビットが「ステージグループ結果」にマッピングされる。このマッピングは、本明細書では「クリーク（clique）マップ」と呼ばれる多数の予めプログラムされたテーブルを使用することで達成される。各クリークマップは、現在のステージ番号とクリークマップに割

り当てられたステージパターン発見ビットのビットに基づいてインデックス付けされる。選択的に、必要とされる「ステージグループ結果ビット」の数がクリークマップの幅よりも大きいときは、クリークマップ内へのインデックス付けはさらに「時間スライス番号」に基づかせることもできる。１つのマップによって提供できるよりも多くのビットが必要な場合は、タイムスライス番号を使用して２以上のマップにアクセスする。代表例においては、３つの１６ビットのマップにアクセスして１つの４８ビットの出力を得る。

【００３２】

各クリークマップに割り当てられるステージ蓄積器結果ビットの数は、速度とメモリ使用との兼ね合いで決まる。３２個のパターン照合ハードウェア実装の場合、通常２または３ビットが用いられ、６４個のパターン照合回路のソフトウェア実装については、８ビットの実装が良好な選択となる。同様に、クリークマップの幅は、通常、速度とメモリ使用との兼ね合いで決まる。

【００３３】

各クリークマップから得られる値はＯＲをとられ、「ステージグループ結果値」を形成する。このステージグループ結果からの幾つかのビットは、任意の数のステージ出力結果を生成するために選択的に使用することができるが、他の方法もステージ出力の生成に使用することができる。また、残りのステージグループ結果ビットは、「ステージグループフィルタ結果」の形成に使用される。ステージグループフィルタ結果はＡＮＤを取られグループ蓄積器に蓄積される。この蓄積器はプロトコルデータ単位の検索の開始時に全て１に初期化される。このグループ蓄積器の値の各ビットは、割り当てられた「グループフィルタ番号」を有する。

【００３４】

グループフィルタは条件を満たしたステージの予め選択されたセットとして指定され、各指定されたステージ内でそのステージ用に指定されたパターンのうちの１つだけが条件を満たすステージについて発見される。プロトコルデータ単位の検索の完了時に、そのグループ蓄積器ビットがセットされかつ適当なステージがプロトコルデータ単位を検索した場合に、グループフィルタは発見されたとみなされる。従来のフィルタ設計を用いる場合と同じく、グループフィルタの発見の結果として、カウント、プロトコルデータ単位の保存、プロトコルデータ単位の廃棄、データ捕捉の開始または停止などの１つまたは複数の動作を他の動作と同様に行なうことができる。

【００３５】

代表例では、本装置は、１つのプロトコル層において最大６４の異なるカプセル化をサポートし、また最大１４個のプロトコル層をサポートすることができる。これは、64^{14}個のフラットフィルタと等価である。本装置に対するフラットフィルタの等価な数は、実装により課される限界であり、本発明の限界ではない。本装置は、ハードウェアまたはソフトウェアで機能を実装することができる。

【００３６】

本明細書に開示される技術は、どの下位層プロトコルが使用されているかを一切知ることなく、上位層のプロトコルにおいてユーザが何かを捜すことができる能力をもたらすものである。また、所望のカプセル化パターンに関する情報を本装置に知らせることによって、本装置は実行時にプロトコルデータ単位におけるカプセル化を識別することができ、これによって、追加のソフトウェアルーチンがその後に各パケットにおけるカプセル化の識別にかかる時間を節約する。本装置をハードウェア及びソフトウェアの両方で実装することで、プロトコルデータ単位を高速に識別することができる。

【００３７】

一般のネットワーク状況では、文字通り数百の異なるノード間を流れるデータが存在し得るが、ユーザがデータを捕捉する対象とするのはそのうち２つからだけである。最新ネットワークの速度と典型的な最新ネットワーク解析器の限られたメモリ空間のために、プロトコルデータ単位の捕捉に割り当てられるバッファ空間はすぐにオーバーランしてしまうおそれがある。従来のシステムでは、捕捉される大多数のプロトコルデータ単位は、ユー

ザが対象としないノードからのものであることもあり得る。一例として、対象となる２つのノードのＩＰ（インターネットプロトコル）アドレスをユーザが知っており、これらの２つのノード間のデータのみを捕捉したいとき、ユーザがネットワークの詳しい知識をもたない場合は、上記の多数のフラットフィルタを自在に操らない限り、プロトコルデータ単位のＩＰアドレスを識別することはできない。しかし、本発明による装置の様々なステージでの識別の能力をもってすれば、プロトコルの識別に必要なものを越える僅かな追加の努力だけで、対象とするこれらのプロトコルデータ単位のフィルタリングが可能となる。

【００３８】

２．ＰＤＵ識別方法

図１は、本発明の様々な代表的な実施形態で説明するプロトコルデータ単位１００の図である。プロトコルデータ単位１００は、データのビット１２０と、１つまたは複数のパケットプロトコルパターン１０５を含む。パケットプロトコルパターン１０５は、本明細書ではカプセル化プロトコルパターン１０５ともコンピュータネットワークプロトコル１０５とも呼ばれ、データをカプセル化するのにコンピュータネットワーク内で用いられたプロトコルを識別する。パケットプロトコルパターン１０５は、カプセル化層とプロトコルデータ単位１００を作成する特定のプロトコルによって定義される。図１は、例示目的だけのものである。プロトコルは、様々の長さを取ることができ、必ずしも図１に示したプロトコルデータ単位内の位置でなくてもよい。

【００３９】

図２は、本発明の様々な代表的な実施形態で説明するプロトコルデータ単位１００の捕捉の図である。図２において、プロトコルデータ単位１００は受信バス２０５で受け取られ、ここでバッファ２１０とも呼ばれる捕捉バッファ２１０内に書き込まれ、プロトコル識別装置２１５によって受け取られる。別の代表的な実施形態では、プロトコルデータ単位１００はプロトコル識別装置２１５によって受信バス２０５上で受け取られ、プロトコル識別装置２１５がプロトコルデータ単位１００を捕捉バッファ２１０へ伝送する。

【００４０】

図３は、本発明の様々な代表的な実施形態で説明する第１のリスト３００である。図４は、本発明の様々な代表的な実施形態で説明するように、第１のリスト３００のエントリ３２０の図である。第１のリスト３００は検索パターン３０５のリストであり、本明細書では検索パターンリスト３００とも呼ばれる。図４に示すように、検索パターンリスト３００の任意の所与のエントリ３２０は、検索パターンインデックス３１０とステージ番号３１５と検索パターン３０５を含む。検索パターンインデックス３１０は、エントリ３２０を識別するインデックスであり、一般に整数である。この例では、検索パターンインデックス３１０は、検索パターン３０５を識別し、第１のエントリについては０、第２のエントリについては１、第３のエントリについては２で始まる。ステージ番号３１５は、検索パターン３０５の検索に用いるステージ３１５を識別する。ステージ番号３１５とステージ３１５自体（どの図にも明示していない）は同じエンティティではないことが認められるが、それらは両方ともステージ３１５の識別に用いられるステージ番号３１５と同じ識別番号（３１５）を用いて参照される。

【００４１】

図３の例では、検索パターンリスト３００の第７エントリ３２０は、それがリストの第７エントリであることを示す、「６」に等しい検索パターンインデックス３１０を持つ。このエントリ３２０は、第２ステージ第３検索パターン３０５を含む。第２ステージ第３検索パターン３０５は、それが第２ステージに関連する検索パターン３０５であることを示す、「２」に等しいステージ番号３１５を有する。この代表例では、プロトコル識別装置２１５は、検索パターン３０５と任意の所与のプロトコルデータ単位１００内で発見されたパケットプロトコルパターン１０５との照合を試みる。特に、装置２１５が全てのステージについて一致を発見するよう試みることを想定している図３により表わされる例については、プロトコル識別装置２１５は、第１ステージ第１検索パターン３０５と、第１ス

テージ第２検索パターン３０５と、第１ステージ第３検索パターン３０５と、第１ステージ第４検索パターン３０５を、分析しているプロトコルデータ単位１００の第１のプロトコルパターン１０５と照合するよう試みる。同様に、プロトコル識別装置２１５は、第２ステージ第１検索パターン３０５と、第２ステージ第２検索パターン３０５と、第２ステージ第３検索パターン３０５を、分析しているプロトコルデータ単位１００の第２のプロトコルパターン１０５と照合するよう試みる。同様に、プロトコル識別装置２１５は、他のステージの第３及び他のあらゆる検索パターン３０５を、分析しているプロトコルデータ単位１００の対応するプロトコルパターン１０５と照合するよう試みる。図３に示した３つの点は、検索パターンリスト３００へ符号化されるあらゆる追加検索パターン３０５を表わしている。装置の制約の範囲内で、検索されるステージ数だけでなく各層についてのパターン数は、一般に実装者により指定され、ユーザの必要に基づいて変化させることができる。検索されるステージ数の他に、各層ごとの最大許容パターン数は、前に述べたように実装に依存する。

【００４２】

図５は、本発明の様々な代表的な実施形態にて説明するように、第１のリスト３００のエントリ３２０の別の図である。別の実施形態では、検索パターン３０５の連続部分３２５が検索パターン３０５から選択され、プロトコルデータ単位１００の検索がそれらを発見するために連続的に行なわれる。例えば、検索パターン３０５の第１の部分３２５が先ず選択され、それについてプロトコルデータ単位が検索される。次に、検索パターン３０５の第２の部分３２５が先ず選択され、それについてプロトコルデータ単位が検索される。このプロセスは、検索パターン３０５の全ての部分３２５が選択されて検索が行なわれるまで継続する。別法では、特定の部分３２５がプロトコルデータ単位１００との照合に失敗した場合に、検索パターン３０５についての検索は終了する。

【００４３】

図６は、本発明の様々な代表的な実施形態にて説明するプロトコルデータ単位１００の識別方法のフローチャートである。ブロック４０５では、プロトコルデータ単位１００が受け取られる。プロトコルデータ単位１００は通常、捕捉バッファ２１０へ書き込まれ、図２に示すようにそれと並行してプロトコル識別装置２１５により捕捉される。プロトコル識別装置２１５がプロトコルデータ単位１００を受け取った後、ブロック４０５は通常ステージ番号が０である開始ステージを選択し、通常プロトコルデータ単位１００の第１バイトであるプロトコルデータ単位１００へのポインタを初期化する。そして、ブロック４０５は制御をブロック４０７へ移す。

【００４４】

ブロック４０７では、グループ結果が初期化される。グループ結果は、完了した全てのステージに対するパターン照合の結果である。一般に、グループ結果は、対応ビット位置に１が置かれる検索パターン３０５の予め選択されたグループについて一致が見つからなかった場合に、各ステージについて検索パターン３０５の予め選択されたグループを表わすビット位置に０を持つビットパターンとなる。このグループ結果は、プロトコルデータ単位１００が予め選択されたプロトコルグループに一致するか否かを判定するのに用いることができる。代表的な実施形態では、一致が見つかった場合、捕捉バッファ２１０内のポインタが動かされ、現在のプロトコルデータ単位１００は捕捉バッファ２１０内に留まる。しかし、一致が見つからない場合は、受け取った次のプロトコルデータ単位１００が現在のプロトコルデータ単位１００を上書きする。そして、ブロック４０７は制御をブロック４０８へ移す。

【００４５】

ブロック４０８では、ステージ結果が初期化される。ステージ結果は、ステージについてのパターン照合の結果である。一般に、この結果は、一致がない各アクティブなステージに関連する各検索パターン３０５を表わすビット位置に０を有し、一致があるときは１を有するビットパターンである。そして、ブロック４０８は制御をブロック４１０へ移す。

【００４６】

ブロック４１０では、プロトコル識別装置２１５は、現在のステージ用の検索パターンリスト３００内のエントリを介して１つまたは複数の検索パターン３０５の次の部分を得る。この照合プロセスは、複数の検索パターン３０５の部分を同時に照合するよう試みることでより効率的に実行される。そして、ブロック４１０は制御をブロック４１５へ移す。

【００４７】

ブロック４１５では、非ゼロのスキップ値（通常、第１ステージの第１の比較ではゼロ）が検索パターン３０５のこの部分３２５へ割り当てられた場合、プロトコルデータ単位１００へのポインタは数バイト進められる。一般に、後の比較について、スキップ値はテーブルから得られる。このテーブルは現在のステージ３１５についてのカプセル化を識別するために検索パターン３０５が必要とする全バイトの知識に基づいて予めプログラムされている。選択的に、プロトコルデータ単位１００の全てのバイトを時間の許す限り比較することも可能である。そして、ブロック４１５は制御をブロック４２０へ移す。

【００４８】

ブロック４２０では、プロトコルデータ単位１００内のパターンが検索パターン３０５のパターンと一致するか否か判定するため、プロトコルデータ単位１００内へポインタを必要なだけ進めて、検索パターン３０５の一部３２５がプロトコルデータ単位１００と比較される。そして、ブロック４２０は制御をブロック４２５へ移す。

【００４９】

ブロック４２５では、ステージ内のその位置に対するステージ結果が形成される。そして、ブロック４２５は制御をブロック４３０へ移す。

【００５０】

ステージを終了させるために指定された検索パターン３０５の１つがプロトコルデータ単位１００内のパターンに一致することが分かると、ブロック４３０は制御をブロック４３５へ移す。見つかった時点で特定のステージを終了させるために指定されたこれらの検索パターンは、「ステージ移行検索パターン」と呼ばれる。一致しなければ、ブロック４３０は制御をブロック４３２へ移す。

【００５１】

プロトコルデータ単位１００の終端に出会うと、ブロック４３２はブロック４３５へ制御を移す。出会わなければ、ブロック４３２は制御をブロック４３３へ移す。

【００５２】

プロトコルデータ単位１００において検索を実行することが必要な現在のステージに、１つまたは複数の検索パターン３０５の残りの部分３２５が存在する場合、ブロック４３３は制御をブロック４１０へ移す。存在しない場合、ブロック４３３は制御をブロック４３５へ移す。

【００５３】

ブロック４３５では、ステージ結果が報告される。ブロック４３５は、そこでブロック４４５へ制御を移す。

【００５４】

ブロック４４５では、完了した全てのステージについてのグループ結果が形成される。そして、ブロック４４５は制御をブロック４５０へ移す。

【００５５】

プロトコルデータ単位１００の終端に出会うと、ブロック４５０は制御をブロック４６０へ移す。出会わなければ、ブロック４５０は制御をブロック４５３へ移す。

【００５６】

プロトコルデータ単位１００において検索を行なう必要のある検索パターン３０５を構成する残りのステージが存在する場合、ブロック４５３は制御をブロック４５５へ移す。存在しない場合、ブロック４５３は制御をブロック４６０へ移す。

【００５７】

ブロック４５５では、検索パターン３０５をプロトコルデータ単位１００内のパケットプロトコルパターン１０５と照合する試みをするための新しいステージが選択される。そし

て、ブロック４５５は制御をブロック４５７へ移す。
【００５８】
ブロック４５７では、プロセスは選択されたステージへ移行する。そして、ブロック４５７は制御をブロック４０８へ移す。
【００５９】
ブロック４６０では、グループ結果が報告される。そして、ブロック４６０はプロセスを終了する。
【００６０】
３．ＰＤＵ識別を行う装置
図７は、本発明の様々な代表的な実施形態にて説明するプロトコルデータ単位１００の識別を行うプロトコル識別装置２１５の図である。図７では、データは制御回路５００により受信バス２０５上で受け取られる。前述しかつ図２に示したように、プロトコルデータ単位１００も代表的な実施形態における並列処理において捕捉バッファ２１０へ書き込まれる。プロトコル識別装置２１５は、プロトコルデータ単位１００内でパケットプロトコルパターン１０５を識別し、識別プロセスの結果に基づいて、捕捉バッファ２１０内に残らないこれらのプロトコルデータ単位１００をフィルタリングし除外する。捕捉バッファ２１０は、例えば、先入れ先出し方式（ＦＩＦＯ）バッファでよい。検索パターンリスト３００の内容に基づいて、制御回路５００は、プロトコルデータ単位１００のどのバイトについて、検索パターン３０５の照合を試みるかを決定する。前述したように、検索パターンリスト３００は、ユーザが一致を得ることを望む検索パターン３０５から構成される。制御回路５００は、検索パターン・グループ一致リスト５１０として図７に示すように、リストやテーブル及び／またはデータベース等からこの情報を得る。
【００６１】
第１ステージのパターン照合の間、プロトコルデータ単位１００と検索が予定されている検索パターン３０５が検索パターン比較器５３０へ送られる。本明細書では、検索パターン比較器５３０は第１の比較器５３０及びパターン比較器５３０とも呼ばれる。制御回路５００は、前述したように、プロトコルデータ単位１００内へのインデックス付けを行なう。
【００６２】
任意の所与のステージが、異なるビットパターン長を有する様々な検索パターン３０５を有し得る。しかし、プロトコルは可変長であるため、ユーザは次のプロトコルまたは次のパケットプロトコルパターンがどこで開始するかについては分からない。ステージ移行パターンとして指定されたパケットプロトコルパターン１０５が所与のカプセル化層について識別されると、装置のステージ部分は見つかったばかりのステージ移行パターンに対して指定されたステージ番号についてリセットされ、プロセスは次のカプセル化層についてパケットプロトコルパターン１０５の検索をすべて初めから開始する。
【００６３】
代表的な実施形態では、検索パターン比較器５３０は、３２個の異なる検索パターン３０５をプロトコルデータ単位１００と同時に照合する能力を有する３２ビット幅のＲＡＭ５３０である。３２ビット幅ＲＡＭ５３０から、プロトコルデータ単位１００がカプセル化された対応するパック済みプロトコルパターン１０５にどの検索パターン３０５が一致したか（もしあれば）を示すビットパターンが、ステージ結果蓄積器５５０（第１の蓄積器５５０とも呼ばれる）へ伝送される。ステージ結果蓄積器５５０（特に図示せず）は、検索パターン３０５がプロトコルデータ単位１００内に見つかったか否かに関する指標を作成する。例えば一致ビット３１が「１」にセットされた場合、探していたパターン番号３１が一致する。「０」は、一致しないことを示す。各ステージについて比較が１回以上行なわれるとすれば、ステージ結果蓄積器５５０は、個々の比較または同時比較の完了の後に更新される。ステージ結果蓄積器５５０に含まれる結果は制御回路５００へ伝送され、さらにステージ－グループマッピング回路５６０（マッピング回路５６０とも呼ばれる）に伝送される。ステージ－グループマッピング回路５６０において、ステージ結果はグル

ープ結果蓄積器５７０（第２の蓄積器５７０とも呼ばれる）へマッピングされ伝送される。グループ結果蓄積器５７０は、検索パターン３０５の予め選択されたグループがプロトコルデータ単位１００内で見つかったか否かに関する指標５７０（特に図示しないが、グループ指標５７０と呼ぶ）を作成する。ステージ－グループマッピング５６０からの出力は制御回路５００にも伝送される。制御回路５００において、それらの出力は、次のステージ番号、次のプロトコルＩＤ、次のプロトコルＩＤの書き込み位置などのステージ結果を他の項目と同様に提供するために用いられる。グループ結果蓄積器５７０は、グループ結果を制御回路５００へ伝送する。所与のステージの完了の後、制御回路５００は、ステージ結果蓄積器５５０をその初期設定へとリセットする。

【００６４】

任意の所与のステージで照合が可能な３２個のパターンが存在し得る。プロトコルデータ単位１００の所与のバイトについて、検索対象である１つまたは複数のパターンを満足する複数の値が存在し得る。そのバイトは、ここで使用するＲＡＭの２５６個のワードのうちの任意のワードを指定することもできる。従って、ＲＡＭはデータの所与のバイトにより指定された２５６個全ての位置についてプログラムされる。バイト値が「０」である場合、いかなるパターンが検索対象であろうとも、ＲＡＭはエントリ０で一致ビットにプログラムされる。バイト値が「１」である場合、それはＲＡＭ内の異なるワードであり、一致ビットの出現を望む方法で、ワードは一致ビットを用いてプログラムされる。従って、単一バイト上で検索することは、これら２５６個の値の任意の組をとり得るパターンを検索することである。２５６個の値のうち対象とするパターンと一致するものはどれでもＲＡＭが選択するようプログラムされていることを保証するのは実装者次第である。

【００６５】

ユーザは、幾つかの異なる型のプロトコルカプセル化を見つけ出し、それらを単一のプロトコルのグループ（例えばＲＦＣ１４９０が後に続きＩＰが後に続くフレームリレー）として識別することに関心があるかもしれない。ユーザは、異なるグループのパターンの発生のカウントを望むかもしれない。ステージ－グループマッピング回路５６０の別の目的は、どのステージを次に調査すべきかを識別することである。例えば、プロトコルデータ単位１００は第１ステージの間にフレームリレーカプセル化として識別され、そして、次のカプセル化がＲＦＣ１４９０であるかまたは他のプロトコル（例えばＬＭＩ）のためのカプセル化であるかを判定するために、第４ステージを用いるように、システムをステージ－グループマッピング回路５６０プログラムすることができる。

【００６６】

プロトコル識別装置２１５は、各カプセル化層について各検索パターン３０５に一致したパケット総数のカウントを維持することができる。加えて、プロトコル識別装置２１５は、カウントの他に、データ捕捉（開始、中心寄せ、停止、記憶、圧縮）を制御する従来のフィルタ関数の作成に用いられる。単独でも組み合わせでも、プロトコルデータ単位１００が満足する任意パターンのプロトコルにより、ユーザの選択で、フラグを設定しかつ／またはそのパターン用に定義されたパラメータを増加させ、あるいは一致が見つかった事実を記録することを可能にする。このような情報は、例えば、プロトコルデータ単位１００と関連するバッファのオーバーヘッド領域に記録することができる。また、いかなるステージも選択的に、プロトコルデータユニット１００に関連するバッファのオーバーヘッド領域の複数の位置のうち１つに値を書き込ませ、そのステージのカプセル化がプロトコルデータ単位１００内で開始された箇所とそのステージについて見つかったプロトコルとを指示させることができる。加えて、プロトコル識別装置２１５は、どのプロトコルがネットワーク上で使用されているかを自動検出したり、プロトコルデータ単位１００をデコードするのに使用することのできるカプセル化情報を提供したり、実行時処理用にパケットの優先順位付けをしたりするのに用いることができる。

【００６７】

制御回路５００は、例えば上記したような対象となる様々な結果を、他の回路や関数に中継するために使用される結果報告回路５８０に伝送する、

多くのデータ処理製品と同じく、本明細書に開示した技術は、ハードウェア要素とソフトウェア要素の組み合わせとして実装される。本発明を使用するために必要な機能は、情報処理装置（例えば、本明細書に開示した技法に従って動作するネットワーク解析器、サーバコンピュータまたはパーソナルコンピュータ）のプログラミングに用いるコンピュータ可読の媒体（例えば、ハードディスク、フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ等）で実現できる。

【００６８】

本明細書に記載した技法はプロトコル解析器において有利に用いることができるが、コンピュータ等のプロトコルデータ単位１００を受信可能な他の装置において使用することもできる。

【００６９】

４．結言

従来技術に対する本発明の実施形態の主要な利点は、プロトコルデータ単位１００とパケットプロトコルパターン１０５との照合に必要となる多数のパターン比較器を大きく低減することである。この低減は、ステージという概念の利用によってもたらされる。さらなる利点は、どの低位層のプロトコルが使用されているかについての知識を持つことなく、高位層のプロトコルにおける特定のパターンを検索する能力である。また、この装置をハードウェアとソフトウェアの両方で実装することで、プロトコルデータ単位を非常に高速で識別するという利点が得られる。他の利点は、特定のプロトコルデータ単位１００内にどのようなカプセル化が存在するかについての情報を提供し、従って後に各パケットを処理するときのソフトウェアルーチン所要時間を節約する能力である。最後に、所望のカプセル化パターンに関する情報をプロトコル識別装置２１５に知らせることにより、プロトコル識別装置２１５は、実行時にプロトコルデータ単位１００をフィルタリングすることができ、これにより、不必要なパケットを後で処理するために追加のソフトウェアルーチンが費やす時間を節約するという利点が得られ、また対象としないプロトコルデータ単位１００を廃棄することで、貴重な捕捉バッファ空間が得られる。

【００７０】

本発明には例として以下の実施形態が含まれる。

【００７１】

（１）プロトコル識別装置により実行可能な指令からなるコンピュータプログラムを具現化して、プロトコルデータ単位（１００）内にデータ（１２０）をカプセル化するのに用いたコンピュータネットワークプロトコル（１０５）を識別する方法ステップを実行する、プロトコル識別装置（２１５）によって読み取り可能な記憶媒体であって、

前記方法ステップは、

データ（１２０）と複数のカプセル化プロトコルパターン（１０５）を含むプロトコルデータ単位を受け取るステップと、

前記プロトコルデータ単位を検索する少なくとも１つのステージ（３１５）が残っている間に、

ａ）残りのステージ（３１５）のうちの１つを選択することと、

ｂ）前記プロトコルデータ単位を検索するための前記選択されたステージのうち少なくとも１つの検索パターン（３０５）が残っている間に、

ｂ１）残りの検索パターン（３０５）のうちの１つを選択することと、

ｂ２）選択された検索パターンを捜して前記プロトコルデータ単位を検索することを繰り返し実行すること、

のａ）及びｂ）を繰り返し実行するステップと、

を含む記憶媒体。

【００７２】

（２）前記方法ステップは、

少なくとも１つのステージ（３１５）が残っている間の繰り返しループの前に、

ｃ）予め定めた検索パターン（３０５）のグループのうち少なくとも１つについてグルー

プ指標（５７０）を割り当てるステップであって、前記グループは少なくとも１つの予め選択された検索パターンを含む少なくとも１つのサブセットを含み、前記予め選択された検索パターンはデータ（１２０）をカプセル化するのに用いる予め選択された少なくとも１つのネットワークプロトコル（１０５）を識別する、ステップと、
ｄ）前記グループ指標を初期化し、少なくとも１つのサブセットがプロトコルデータ単位内の予想された位置に存在することを指定するステップと、をさらに含み、
プロトコルデータ単位を検索するための前記選択されたステージの少なくとも１つの検索パターンが残っている間の繰り返しループの後に、
前記選択されたステージについてのグループの各サブセットに関連する全ての検索パターンがプロトコルデータ単位の予想された位置に存在しない場合、そのグループの全サブセットがプロトコルデータ単位に存在しないことを指定するように、前記グループ指標を設定するステップをさらに含む、
上記(１)に記載の記憶媒体。

【００７３】

（３）前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップに続いて、前記方法ステップは、
少なくとも１つのステージが残っている間の繰り返しループの後に、
プロトコルデータ単位内の予想された位置に少なくとも１つのサブセットが存在する場合、そのプロトコルデータ単位をバッファ（２１０）に配置するステップをさらに含む、
上記(２)に記載の記憶媒体。

【００７４】

（４）前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップは、
プロトコルデータ単位を検索する選択されたステージの検索パターンの少なくとも一部（３２５）が残っている間に、
ｅ）選択された検索パターンの残っている未検索部分のうちの１つを選択するステップと、
ｆ）選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
を繰り返し実行することをさらに含む、上記(１)に記載の記憶媒体。

【００７５】

（５）前記方法ステップは、
前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが前記プロトコルデータ単位内の選択部分を見つけられなかった場合、
ｇ）プロトコルデータ単位を検索する前記選択されたステージの検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップと、
ｈ）プロトコルデータ単位を検索する前記選択されたステージの少なくとも１つの検索パターンが残っている間の繰り返しループを抜け出すステップと、
をさらに含む、上記(４)に記載の記憶媒体。

【００７６】

（６）前記残っている検索パターンの１つを選択するステップに続いて、前記方法ステップは、
プロトコルデータ単位を検索する前記選択されたステージの少なくとも１つの他の検索パターンが残っている場合、
ｉ）前記他の残っている検索パターンのうち少なくとも１つを選択するステップと、
ｊ）前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンを捜してプロトコルデータ単位を検索するステップと、
をさらに含む、上記(１)に記載の記憶媒体。

【００７７】

（７）前記選択された検索パターンを捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンを捜してプロトコルデータ単位を検索するステップは、
プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部と、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部とが残っている間に、
ｋ）前記選択された検索パターンの残っている未検索部分の１つを選択するステップと、
ｌ）前記他の選択された検索パターンの残っている未検索部分の１つを選択するステップと、
ｍ）選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
ｎ）前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと並行して、前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
をさらに含み、
あるいは、プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部が残っている間に、
ｏ）前記選択された検索パターンの残っている未検索部分の１つを選択するステップと、
ｐ）選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
を繰り返し実行することをさらに含み、
あるいは、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部が残っている間に、
ｑ）前記他の選択された検索パターンの残っている未検索部分の１つを選択するステップと、
ｒ）前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップと、
を繰り返し実行することをさらに含む、
上記(６)に記載の記憶媒体。

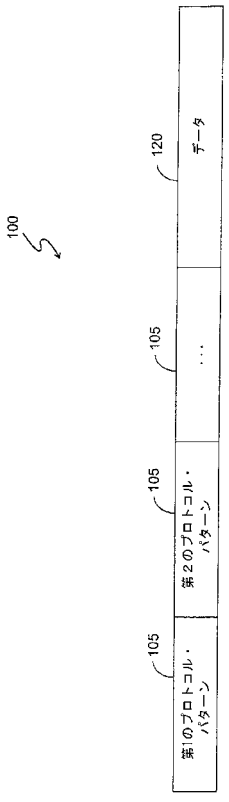
【００７８】

（８）前記方法ステップは、
前記選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に選択された検索パターンの選択部分を見つけられなかった場合、及び、前記他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索する並行ステップが、プロトコルデータ単位内に他の選択された検索パターンの選択部分を見つけられなかった場合に、
プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部と、プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部とが残っている間の繰り返しループを抜け出すステップをさらに含み、
あるいは、選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に選択された検索パターンの選択部分を見つけられなかった場合、
プロトコルデータ単位を検索する選択されたステージの選択された検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップをさらに含み、
あるいは、他の選択された検索パターンの選択部分を捜してプロトコルデータ単位を検索するステップが、プロトコルデータ単位内に他の選択された検索パターンの選択部分を見つけられなかった場合、
プロトコルデータ単位を検索する選択されたステージの他の選択された検索パターンの少なくとも一部が残っている間の繰り返しループを抜け出すステップをさらに含む、

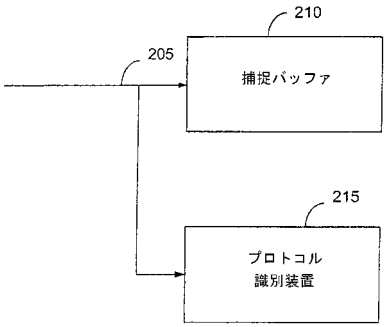
上記(７)に記載の記憶媒体。
【００７９】
（９）プロトコルデータ単位内でデータ（１２０）をカプセル化するのに用いるコンピュータネットワークプロトコル（１０５）を識別する装置であって、
プロトコルデータ単位（１００）を受け取ることができ、複数のステージ（３１５）のそれぞれについて、データのカプセル化に用いるネットワークプロトコルの１つを識別する少なくとも１つの検索パターン（３０５）を得ることができる、制御回路（５００）と、前記制御回路に接続され、該制御回路からプロトコルデータ単位を受け取ることができるパターン比較器（５３０）であって、前記制御回路は個々のステージを連続的に選択することができ、該選択されたステージについて、前記制御回路から選択されたステージの少なくとも１つの検索パターンを受け取り、受け取った検索パターンを捜してプロトコルデータ単位を別々に検索することができるパターン比較器と、
を備える装置。
【００８０】
（１０）前記パターン比較器に接続され、前記選択されたステージの検索から結果を蓄積することができる第１の蓄積器（５５０）をさらに備える、上記(９)に記載の装置。
【００８１】
本発明を好適な実施形態に関して詳しく説明したが、説明した実施形態は一例として示したものであり、限定として示したものではない。当業者は、上記実施形態に様々な変形を加えて、特許請求の範囲内に含まれる等価な実施形態とすることができることを理解するであろう。
【図面の簡単な説明】
【図１】本発明の様々な代表的な実施形態で説明するプロトコルデータ単位の図である。
【図２】本発明の様々な代表的な実施形態で説明するプロトコルデータ単位捕捉の図である。
【図３】本発明の様々な代表的な実施形態で説明する第１のリストの図である。
【図４】本発明の様々な代表的な実施形態で説明する第１のリストのエントリの図である。
【図５】本発明の様々な代表的な実施形態で説明する第１のリストのエントリの他の図である。
【図６】本発明の様々な代表的な実施形態で説明するプロトコルデータ単位の識別方法のフローチャートである。
【図７】本発明の様々な代表的な実施形態で説明するプロトコルデータ単位識別用のプロトコル識別装置の図である。
【符号の説明】
１００　プロトコルデータ単位
１０５　プロトコルパターン
１２０　データ
２０５　受信バス
２１０　捕捉バッファ
２１５　プロトコル識別装置
３００　検索パターンリスト
３０５　検索パターン
３１０　検索パターンインデックス
３１５　ステージ
３２０　エントリ
３２５　選択部分
５００　制御回路
５１０　検索パターン兼グループ一致リスト
５３０　パターン比較器

５５０　ステージ結果蓄積器
５６０　マッピング回路
５７０　グループ指標
５８０　結果報告回路

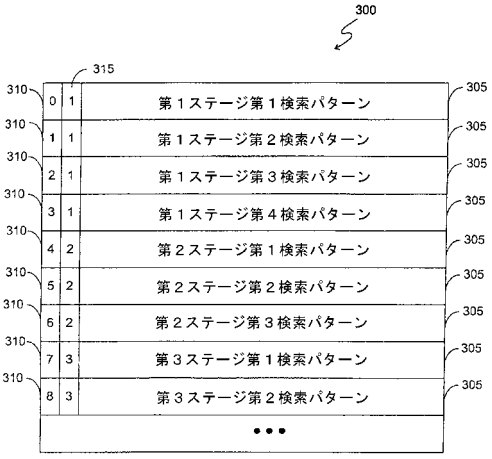
【図１】



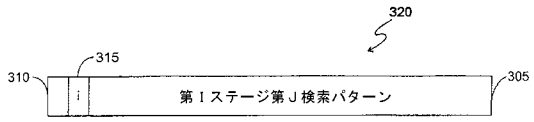
【図２】



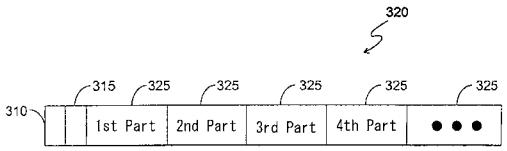
【図３】



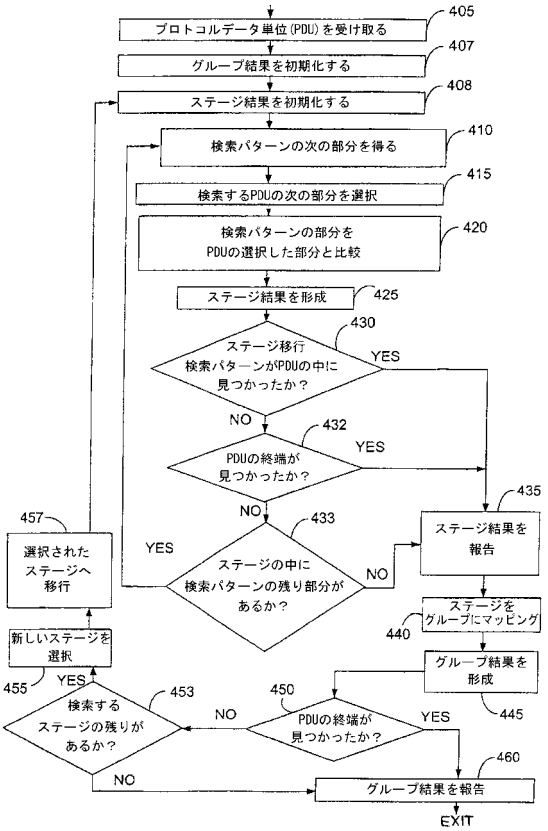
【図４】


320
315
310
i
第ｉステージ第Ｊ検索パターン
305

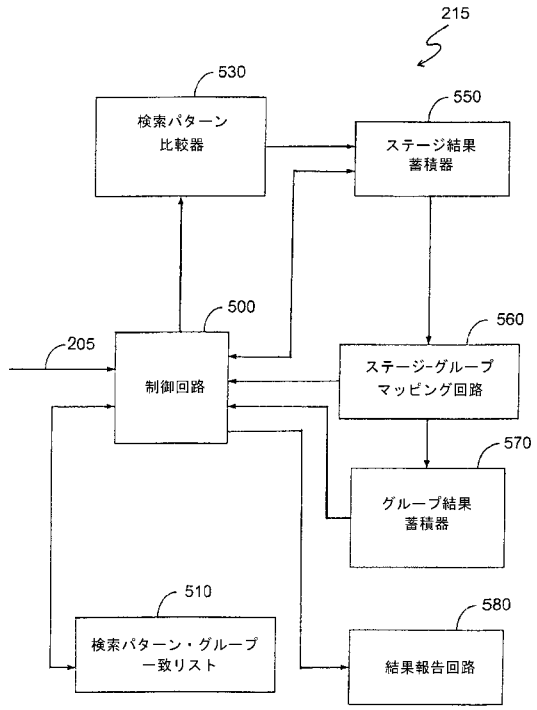
【図５】


320
315
325
325
325
325
325
310
1st Part
2nd Part
3rd Part
4th Part

【図６】


プロトコルデータ単位(PDU)を受け取る
405
グループ結果を初期化する
407
ステージ結果を初期化する
408
検索パターンの次の部分を得る
410
検索するPDUの次の部分を選択
415
検索パターンの部分を
PDUの選択した部分と比較
420
ステージ結果を形成
425
ステージ移行
検索パターンがPDUの中に
見つかったか？
430
YES
NO
PDUの終端が
見つかったか？
432
YES
NO
ステージの中に
検索パターンの残り部分が
あるか？
433
YES
NO
選択された
ステージへ
移行
457
ステージ結果を
報告
435
ステージを
グループにマッピング
440
新しいステージを
選択
グループ結果を
形成
445
検索する
ステージの残りが
あるか？
455
YES
453
NO
PDUの終端が
見つかったか？
450
YES
NO
グループ結果を報告
460
EXIT

【図７】


215
530
検索パターン
比較器
550
ステージ結果
蓄積器
500
205
制御回路
560
ステージ-グループ
マッピング回路
570
グループ結果
蓄積器
510
検索パターン・グループ
一致リスト
580
結果報告回路

フロントページの続き

(72)発明者　ヴォン・ブラック
アメリカ合衆国８０９２０コロラド州コロラド・スプリングス、モスミル・コート　１００１０

審査官　安藤　一道

(56)参考文献　米国特許第０５８５０３８８（ＵＳ，Ａ）
特開２００１－１７７５９５（ＪＰ，Ａ）
特開平１０－１７３７０８（ＪＰ，Ａ）
特開平０７－３２１７９４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 29/04