(19) österreichisches patentamt

(10) **AT 523933 B1 2022-01-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 51010/2020
(22) Anmeldetag: 18.11.2020
(45) Veröffentlicht am: 15.01.2022

(51) Int. Cl.: ***G06F 21/55*** (2013.01)
G06F 21/56 (2013.01)
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 29/06 (2006.01)

(56) Entgegenhaltungen:
WO 0184285 A2
F. CUPPENS, A. MIEGE: "Alert correlation in a cooperative intrusion detection framework." In: 2002 IEEE Symposium on Security and Privacy, 2002. Konferenzbeitrag. IEEE, Berkeley, CA, USA, 12.-15. Mai 2002 (12.02.2002), Seiten 202-215. doi: 10.1109/SECPRI.2002.1004372
JP 2002342276 A
US 2004111637 A1
JP 2004336130 A
US 2005076245 A1
US 2006259968 A1
R. VAARANDI: "Real-time classification of IDS alerts with data mining techniques." In: 2009 IEEE Military Communications Conference, MILCOM 2009. Konferenzbeitrag. IEEE, Boston, MA, USA, 18.-21. Jänner 2009 (18.01.2009), Seiten 1-7. doi: 10.1109/MILCOM.2009.5379762
US 9225730 B1

(73) Patentinhaber:
AIT Austrian Institute of Technology GmbH
1210 Wien (AT)

(72) Erfinder:
Landauer Max
1070 Wien (AT)
Skopik Florian DDr.
2000 Stockerau (AT)
Wurzenberger Markus Dr.
1020 Wien (AT)

(74) Vertreter:
Wildhack & Jellinek Patentanwälte OG
1030 Wien (AT)

(54) **Verfahren zur Klassifizierung von anomalen Betriebszuständen eines Computernetzwerks**

(57) Die Erfindung betrifft ein Verfahren zur Klassifizierung von anomalen Betriebszuständen eines Computernetzwerks (1),

- wobei auf den Computern ein Angriffserkennungssystem (S_A, S_B) zur Erkennung von anomalen Betriebszuständen abläuft, wobei das Angriffserkennungssystem dazu ausgebildet ist, bei Eintreten von anomalen Betriebszuständen Alarmobjekte (AO; AO_1, ..., AO_n) zu erstellen,
- wobei die einzelnen Alarmobjekte zu Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zusammengefasst werden,
- wobei die einzelnen Alarmobjektgruppen verglichen und nach einer vorgegebenen Aggregationsmetrik zu Alarmobjektmustern (P; P_1, ..., P_k) zusammengefasst werden,
- wobei den Alarmobjektmustern (P; P_1, ..., P_k) jeweils repräsentative Alarmobjekte (RA; RA_1, ..., P_l) zugewiesen werden,
- wobei jedem Alarmobjektmuster (P; P_1, ..., P_k) ein Angriffstyp zugeordnet wird, und
- diejenigen Betriebszustände als anomale Betriebszustände erkannt werden, die auf denjenigen Angriffstyp zurückzuführen sind, der dem jeweiligen Alarmobjektmuster (P; P_1, ..., P_k) zugeordnet ist.

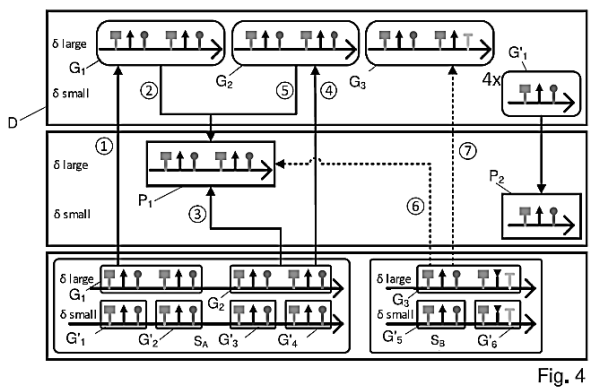


Fig. 4

AT 523933 B1 2022-01-15

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Klassifizierung von anomalen Betriebszuständen eines Computernetzwerks, die auf Variationen unterschiedlicher Angriffstypen zurückzuführen sind, gemäß dem Oberbegriff von Patentanspruch 1.

[0002] Angriffserkennungssysteme sind automatisierte Programme, die das Systemverhalten nach vorgegebenen Regeln beobachten und mithilfe spezifisch konfigurierter Detektoren analysieren und in Fall einer Detektion eines Angriffs oder einer Fehlfunktion des Computersystems Alarme bzw. Alarmobjekte erstellt. Angriffserkennungssysteme werden in verschiedensten Netzwerk- und Systemumgebungen eingesetzt, um z.B. Cyber-Angriffe frühzeitig zu erkennen und zu verhindern.

[0003] In vielbenützten Systemen ist die Anzahl der Alarme sowohl durch ständige Angriffe - etwa aus dem Internet durch automatisierte Skripte oder Bots - als auch normales Benutzerverhalten, das Fehlalarme auslösen kann, oft immens. Dazu ist es meist nicht möglich, einen Alarm einem bestimmten Angriff zuzuordnen, da:

- Aktionen, die möglicherweise Alarme auslösen, nicht nur einen einzigen Alarm spezifisch für diese Aktion auslösen, sondern meist eine Reihe von Alarmen auslösen.
- Jeder dieser ausgelösten Alarme auch bei anderen Aktionen auftreten könnte, zum Beispiel als Teil der dabei entstehenden Alarme. Dies wird dadurch bekräftigt, dass es im Allgemeinen von Interesse ist, möglichst generische Regeln und Detektoren zur Erkennung von Angriffen zu entwerfen, um so auch noch unbekannte Angriffstechniken oder Varianten von Angriffen mit möglichst großer Wahrscheinlichkeit erkennen zu können.
- Auch bei Auftreten derselben Aktion nicht garantiert ist, dass exakt die gleichen Alarme ausgelöst werden, sondern diese sich in ihren Attributen, Reihenfolgen, oder Auftrittszeitpunkten unterscheiden können.
- Gleiche oder ähnliche Angriffe mit unterschiedlichen Konfigurationen ausgeführt werden können, wodurch sich deren Manifestationen in den beobachteten Systemdaten ändert und somit auch die resultierenden Alarme beeinflusst werden.
- Sich Mischungen aus mehreren Angriffen oder auch Fehlalarmen, die zufällig gleichzeitig auftreten, ergeben können.
- Eine Zuordnung eine vom Menschen durchgeführte semantische Bearbeitung bedarf, diese jedoch im Allgemeinen Fall bei unterschiedlichen Systemumgebungen jeweils spezifisch durchgeführt werden müsste, und es somit keine generell gültige Regelbasis für das Zuordnen von Alarmen zu Angriffen gibt.

[0004] Im derzeitigen Stand der Technik existiert jedoch kein Ansatz, der es erlaubt, auftretende Alarme, deren Struktur bzw. beinhaltete Attribute unbekannt sind, spezifischen Angriffstechniken zuzuordnen. Existierende Ansätze basieren ausschließlich auf dem Finden von vordefinierten Werten in verschiedenen Alarmen. Dabei werden vor allem IP-Adressen verwendet, um Verbindungen zwischen Alarmen herzustellen (siehe z.B. Cuppens, F., & Miege, A. (2002, May). Alert correlation in a cooperative intrusion detection framework. In Proceedings 2002 IEEE symposium on security and privacy (pp. 202-215). IEEE), oder die Gruppierung basiert ausschließlich auf wenigen vordefinierten Attributen aus dem IDMEF Format (siehe z.B. Risto Vaarandi. 2009. Real-time classification of IDS alerts with data mining techniques. In MILCOM 2009-2009 IEEE Military Communications Conference. IEEE, 1-7). Dies ist jedoch vor allem bei host-basierten Systemen nicht möglich, da manche Attribute (IP-Adressen, Ports) nicht notwendigerweise in den Protokollzeilen vorhanden sind, sowie auf Systemen, wo aufgrund von Virtualisierung und Containerisierung Netzwerkadressen keine eindeutigen Zuordnungen erlauben. Weiters lassen sich Muster, die auf dem Vorkommen bestimmter systemspezifischer Attribute wie IP-Adressen beruhen, nur schwer auf ein allgemeines dezentralisiertes Netzwerk generalisieren, wo das Erstellen von Verbindungen basierend auf gleichen IP-Adressen nicht möglich ist.

[0005] Aufgabe der Erfindung ist es daher, ein Verfahren bereitzustellen, das es ermöglicht, die von Angriffserkennungssystemen erstellten Alarme bzw. Alarmobjekte automatisiert einzelnen

Angriffstypen zuzuordnen, sodass die Anzahl an Alarmen bzw. Alarmobjekten, die manuell überprüft werden müssen, effektiv reduziert werden kann.

[0006] Die Erfindung löst diese Aufgabe bei einem Verfahren gemäß dem Oberbegriff des Patentanspruchs 1 mit den kennzeichnenden Merkmalen des Patentanspruchs 1. Erfindungsgemäß ist dabei vorgesehen,

- dass die einzelnen Alarmobjekte der Alarmobjektsequenz zu Alarmobjektgruppen zusammengefasst werden,
- dass die einzelnen Alarmobjektgruppen basierend auf der Reihenfolge, der Häufigkeit und/oder den Attributen der den jeweiligen Alarmobjektgruppen zugeordneten Alarmobjekte nach einer vorgegebenen Ähnlichkeitsmetrik hinsichtlich ihrer Ähnlichkeit verglichen und unter Vorgabe eines Alarmobjektgruppen-Ähnlichkeitsschwellenwerts aufgrund deren Ähnlichkeit nach einer vorgegebenen Aggregationsmetrik zu Alarmobjektmustern in Form von Datenobjekten zusammengefasst werden,
  wobei den Alarmobjektmustern jeweils repräsentative Alarmobjekte zugewiesen werden, die diejenigen Alarmobjekte, insbesondere deren Attribute und Werte, die den als ähnlich erkannten Alarmobjektgruppen zugeordnet sind, repräsentieren und
  wobei jedem Alarmobjektmuster ein Angriffstyp zugeordnet wird, und
- dass diejenigen anomalen Betriebszustände, die denjenigen Alarmobjekten zugrunde liegen, die den zu einem jeweiligen Alarmobjektmuster zusammengefassten Alarmobjektgruppen zugeordnet sind, als anomale Betriebszustände erkannt werden, die auf denjenigen Angriffstyp zurückzuführen sind, der dem jeweiligen Alarmobjektmuster zugeordnet ist.

[0007] Das erfindungsgemäße Verfahren ermöglicht es vorteilhafterweise, von Angriffserkennungssystemen erzeugten Alarmobjekte durch die Erstellung von Alarmobjektmustern einzelnen Angriffen bzw. Angriffstypen zuzuordnen. Auf diese Weise kann eine effektive Reduktion der Anzahl der Alarmobjekte, die von Menschen gesichtet werden müssen, sowie eine semantische Anreicherung mit Angriffsinformationen und automatische Klassifizierung erzielt werden. Dabei werden Alarmobjektmuster durch Aggregation von Einzelalarmobjekten bzw. Alarmobjektgruppen gebildet.

[0008] Diese Vorgehensweise bringt unter anderem folgende Vorteile mit sich:

- Reduktion der Alarmobjekte, die vom Menschen gesichtet und interpretiert werden müssen.
- Wiederverwendbarkeit der Alarmobjektmuster, um gleiche oder ähnliche Angriffe auf anderen Systemen erkennen zu können.
- Geringere Wahrscheinlichkeit einer Fehlinterpretation des Menschen durch zusätzliche Information, da ähnliche Alarmobjektmuster bereits in vergangenen Situationen gefunden wurden.
- Verbesserungen der existierenden Erkennungsregeln und Detektoren.

[0009] Unter Angriffserkennungssystemen werden im Zusammenhang mit der Erfindung automatisierte Programme zur automatisierten Analyse des Systemverhaltens von Computern bzw. Computernetzwerken verstanden.

[0010] Angriffserkennungssysteme werden in verschiedensten Netzwerk- und Systemumgebungen eingesetzt, um z.B. Cyber-Angriffe frühzeitig zu erkennen und zu verhindern. Angriffserkennungssysteme sind automatisierte Programme, die das Systemverhalten beispielsweise nach vorgegebenen Regeln beobachten und mithilfe spezifisch konfigurierter Detektoren analysieren, oder sicherheitsrelevante Ereignisse an dafür zuständige Analysekomponenten weiterleiten.

[0011] Dabei kann zwischen signaturbasierten Angriffserkennungssystemen, die nach vorgegebenen Mustern suchen, die bekanntermaßen auf Angriffe auf bzw. Manipulation des Computers bzw. Computernetzwerks hindeuten, zum Beispiel eine bestimmte Zeichenkette, und anomaliebasierten Angriffserkennungssystemen, die mithilfe von selbstlernenden Methoden ein Basisverhalten der Systemumgebung erstellen und Abweichungen von diesem Grundverhalten als möglichen Angriff kennzeichnen und melden, unterschieden werden.

[0012] Weiters kann zwischen netzwerkbasierten Angriffserkennungssystemen, die den Datenverkehr zwischen einer Menge an Netzwerkkomponenten, wie zum Beispiel Computern, Routern,

Switches oder Firewalls, analysieren, und host-basierten Angriffserkennungssystemen, die Ereignisse auf einer einzelnen Netzwerkkomponente, die zum Beispiel in Protokolldaten und sicherheitsrelevanten Monitoring Daten abgebildet werden, analysieren, unterschieden werden.

[0013] Unabhängig vom Typ des Angriffserkennungssystems führen die durch die automatische Analyse als für die weitere Bearbeitung relevant, anomal, oder anderweitig als potentiell gefährlich erkannten Ereignisse oder Aktivitäten zu einer Erzeugung eines Alarmobjekts, das spezifische Informationen über das Angriffserkennungssystem, das analysierte Ereignis, sowie den Kontext (z.B. Uhrzeit, vorhergehende Ereignisse, andere mit dem Ereignis zusammenhängende Ereignisse, die auch möglicherweise aus unterschiedlichen Datenquellen stammen können) des Auftreten dieses Ereignisses umfasst, und an ein weiteres System, insbesondere ein Sicherheitssystem das zur Aufbereitung von Alarmobjekten für die Kontrolle und Bearbeitung durch einen Menschen entwickelt wurde, weitergeleitet wird.

[0014] Je nach Systemvoraussetzungen können verschiedenste Angriffserkennungssysteme parallel verwendet werden, die jeweils unterschiedliche Konfigurationen aufweisen. Da es keine Standardisierung von Alarmen gibt, bzw. jeder Versuch einer Standardisierung bzw. Vereinheitlichung (zum Beispiel IDMEF Standard in RFC4765) zu einem Verwerfen von möglicherweise wesentlichen Attributen eines Alarmobjekts führt, hat dies zur Folge, dass bei unterschiedlichen Arten von Angriffen bzw. Angriffsversuchen, unterschiedlich strukturierte Alarmobjekttypen erstellt werden, die jeweils über bestimmte nicht-einheitliche Attribute verfügen.

[0015] Die Unterscheidungen der Alarmtypen kann über eine Vielzahl von Aspekten erfolgen, zum Beispiel über einem Alarmobjekt zugeordnete Attribute, zum Beispiel Auftrittszeitpunkt, Information des Detektors oder der verletzten Regel, der zur Verletzung der Regel geführte Wert, Ereignisinformationen, verdächtige und weitere unverdächtige Parameter des Ereignisses, Systemmesswerte, Ordnerstrukturen, betroffene Programme, Vorklassifizierungen durch das Angriffserkennungssystem, etc. Weiters sind die von Angriffen bzw. Angriffsversuchen ausgelösten Sequenzen von Alarmobjekten Variationen unterworfen, wie etwa die Reihenfolge des Auftretens der Alarmobjekte, das Vorhandensein von zusätzlichen Alarmobjekten, dem Ausbleiben von Alarmobjekten in Alarmobjektsequenzen, die relativen Auftrittszeitpunkte der Alarmobjekte, etc.

[0016] Unter einem Erkennungsfall im Zusammenhang mit der Erfindung wird verstanden, wenn ein Angriffserkennungssystem, das z.B. über eine Anzahl an Regeln oder selbstlernenden Detektoren verfügt und eine Anzahl an Datenquellen, die z.B. kontinuierlich netzwerkbasierte oder host-basierte Daten zur Verfügung stellen, analysiert, eine Verletzung einer Regel, ein Auftreten eines bestimmten vordefinierten Musters, eine Erkennung eines sicherheitsrelevanten Ereignisses, oder ein anderweitiges ungewöhnliches Abweichen vom als normal angesehenen Verhalten eines Computers bzw. Computersystems feststellt, und daraufhin ein Alarmobjekt oder mehrere Alarmobjekte erzeugt, das oder die an zur Verfügung gehalten oder an andere Systeme weitergeleitet werden können.

[0017] Unter einem Alarmobjekt wird im Zusammenhang mit der Erfindung ein von einem Angriffserkennungssystem aufgrund eines Erkennungsfalls generiertes semi-strukturiertes Objekt verstanden, das eines oder mehrere Attribute umfasst, wobei die den jeweiligen Attributen zugehörigen Werte aus Zahlen, Zeichenketten, komplexen Datentypen wie IP Adressen, Listen solcher Werte, oder anderen semi-strukturierten Objekten bestehen können, und die Anzahl und Ausprägung der Attribute je nach Angriffserkennungssystem und Erkennungsfall unterschiedlich sein können.

[0018] Unter einer Alarmobjektsequenz im Zusammenhang mit der Erfindung wird eine Abfolge von nach deren zeitlichem Auftreten geordneten Alarmobjekten verstanden, wobei die Alarmobjektsequenzen aufgrund der zeitlichen Nähe und logischen Zusammengehörigkeit der Alarmobjekte unterteilt werden können.

[0019] Eine Alarmobjektgruppe im Zusammenhang mit der Erfindung umfasst eine Anzahl von Alarmobjekten, d.h. eine Teilsequenz einer Alarmobjektsequenz, die z.B. aufgrund der zeitlichen Nähe und/oder logischen Zusammengehörigkeit der Alarmobjekte gebildet wurde.

[0020] Unter einem Alarmobjektmuster wird im Zusammenhang mit der Erfindung eine Alarmobjekt- „Übergruppe“ verstanden, die repräsentativ für eine Menge an Alarmobjektgruppen gebildet wird. Das Alarmobjektmuster selbst ist jedoch nicht Teil dieser Menge. Das Alarmobjektmuster stellt die Gesamtheit der repräsentierten Alarmobjektgruppen möglichst gut darstellt bzw. wird so gebildet, dass es eine möglichst hohe Ähnlichkeit zu jeder der einzelnen, der Menge zugehörigen, Alarmobjektgruppen aufweist.

[0021] Eine besonders effektive Zuordnung von Alarmobjekten zu Alarmobjektgruppen kann erzielt werden,

- wenn die einzelnen Alarmobjekte der Alarmsequenz nach der zeitlichen Nähe des Zeitpunkts ihrer Erstellung, insbesondere unter Vorgabe eines zeitlichen Abstandsschwellenwerts, zu Alarmobjektgruppen zusammengefasst werden,

und/oder

- wenn die einzelnen Alarmobjekte der Alarmsequenz nach der Ähnlichkeit der den Alarmobjekten zugeordneten Attribute zu Alarmobjektgruppen zusammengefasst werden.

[0022] Um zu erzielen, dass jedes Alarmobjekt jeweils mehreren Alarmobjektgruppen zugeordnet wird, kann dabei insbesondere vorgesehen sein, dass eine Anzahl unterschiedlicher zeitlicher Abstandsschwellenwerte gleichzeitig für die Zusammenfassung zu Alarmobjektgruppen herangezogen werden.

[0023] Um sicherzustellen, dass die Alarmobjektmuster basierend auf einer robusten und repräsentativen Auswahl von Alarmobjektgruppen erstellt werden, kann vorgesehen sein, dass eine Datenbank angelegt wird, wobei in der Datenbank die erstellten Alarmobjektgruppen und Alarmobjektmuster, sowie die Zugehörigkeit der einzelnen Alarmobjektgruppen zu den einzelnen Alarmobjektmustern hinterlegt werden.

[0024] Eine weitere Verbesserung der Repräsentativität der Alarmobjektmuster basierend kann erzielt werden,

- wenn die einzelnen Alarmobjektgruppen nach deren Erstellung in der Datenbank hinterlegt werden, und
- wenn die Alarmobjektmuster auf Grundlage der in der Datenbank hinterlegten Alarmobjektgruppen erstellt werden, wobei insbesondere vorgesehen ist, dass, im Fall, dass die Datenbank nur eine einzige Alarmobjektgruppe enthält, ein Alarmobjektmuster erstellt wird, dessen repräsentative Alarmobjekte den Alarmobjekten der einzigen Alarmobjektgruppe entsprechen, insbesondere mit den Alarmobjekten der einzigen Alarmobjektgruppe identisch sind.

[0025] Um bei einem erfindungsgemäßen Verfahren die Datenbank besonders übersichtlich und kompakt zu gestalten, kann vorgesehen sein, dass die Zugehörigkeit der einzelnen Alarmobjektgruppen zu den einzelnen Alarmobjektmustern in Form von Listen umfassend die einem jeweiligen Alarmobjektmuster zugeordneten Alarmobjektgruppen in der Datenbank hinterlegt wird,
wobei Listen zumindest eines der folgenden Typen angelegt werden:

- unbeschränkte Listen,
- linear befüllbare Listen,
- logarithmisch befüllbare Listen, und

wobei insbesondere vorgesehen ist, dass die Wahrscheinlichkeit einer Ersetzung eines Elements einer logarithmisch befüllbaren Liste mit absteigender Position des Elements in der logarithmisch befüllbaren Liste abnimmt.

[0026] Besonders effizient kann die Ähnlichkeit der Alarmobjekte der einzelnen Alarmobjektgruppen untereinander und/oder die Ähnlichkeit neu erstellter Alarmobjektgruppen mit den bereits erstellten Alarmobjektmustern ermittelt werden, wenn die Ähnlichkeit der Alarmobjekte der einzelnen Alarmobjektgruppen und/oder für neu erstellte Alarmobjektgruppen die Ähnlichkeit mit den bereits erstellten Alarmobjektmustern berechnet wird, indem nach übereinstimmenden Attributen und/oder übereinstimmenden, den Attributen zugeordneten, Werten gesucht wird.

[0027] Eine Gesamtähnlichkeit der Alarmobjekte innerhalb einer Alarmobjektgruppe kann auf besonders einfache Weise ermittelt werden,

- wenn alle Attribute der hinsichtlich ihrer Ähnlichkeit zu analysierenden Alarmobjekte miteinander verglichen werden und jeweils die Anzahl der Übereinstimmungen und der Unterschiede der den jeweiligen Attributen zugeordneten Werte ermittelt werden und
- wenn eine Gesamtähnlichkeit der Alarmobjekte innerhalb einer Alarmobjektgruppe als Verhältnis der ermittelten Übereinstimmungen zur Summe der Übereinstimmungen und Unterschiede ermittelt wird.

[0028] Eine besonders effiziente Vorgehensweise zur Zusammenfassung bzw. Aggregation von Alarmobjektgruppen zu Alarmobjektmustern kann bereitgestellt werden, wenn die als ähnlich erkannten Alarmobjektgruppen zu Alarmobjektmustern zusammengefasst werden, indem
- nach einer vorgegebenen Ähnlichkeitsmetrik nach übereinstimmenden Alarmobjekten in den einzelnen als ähnlich erkannten Alarmobjektgruppen gesucht wird, und
- die einzelnen übereinstimmenden Alarmobjekte zusammengefasst werden, indem jeweils die als übereinstimmend erkannten Attribute der übereinstimmenden Alarmobjekte herangezogen werden und ausgewählte, insbesondere alle, Werte, die den als übereinstimmend erkannten Attributen in den jeweiligen Alarmobjekten zugeordnet sind, gemeinsam mit dem jeweiligen Attribut im entsprechenden repräsentativen Alarmobjekt des Alarmobjektmusters hinterlegt werden.

[0029] Eine besonders effiziente Vorgehensweise zur Erstellung von repräsentativen Alarmobjekten von Alarmobjektmustern kann bereitgestellt werden, wenn beim Zusammenfassen der einzelnen übereinstimmenden Alarmobjekte der Alarmobjektgruppen zu Alarmobjektmustern
- Listen umfassend ausgewählte, insbesondere alle, Werte, die einem als übereinstimmend erkannten Attribut in den jeweiligen übereinstimmenden Alarmobjekten zugeordnet sind, gemeinsam mit dem jeweiligen Attribut im jeweils entsprechenden repräsentativen Alarmobjekt des Alarmobjektmusters hinterlegt werden und/oder
- Platzhalter für die Werte, die einem als übereinstimmend erkannten Attribut in den jeweiligen übereinstimmenden Alarmobjekten zugeordnet sind, im jeweils entsprechenden repräsentativen Alarmobjekt des Alarmobjektmusters hinterlegt werden, wenn die Anzahl an unterschiedlichen Werten, die das jeweilige Attribut in den jeweiligen Alarmobjekten annimmt, einen vorgegebenen Maximalwert überschreitet.

[0030] Eine besonders effiziente Vorgehensweise zur Suche nach übereinstimmenden Alarmobjekten in den Alarmobjektgruppen kann bereitgestellt werden, wenn die Ähnlichkeitsmetrik für die Suche nach übereinstimmenden Alarmobjekten in den Alarmobjektgruppen auf zumindest einer der folgenden Vorgehensweisen beruht:
a) dass die den Alarmobjektgruppen zugeordneten Alarmobjekte jeweils paarweise hinsichtlich deren Ähnlichkeit miteinander verglichen werden, und dass diejenigen Alarmobjektpaare ermittelt werden, deren Ähnlichkeit am größten ist, wobei insbesondere vorgesehen ist, dass jedes Alarmobjekt nur in einem Alarmobjektpaar enthalten ist,
b) dass zunächst innerhalb der einzelnen Alarmobjektgruppen die Häufigkeiten der einzelnen zugeordneten Alarmobjekte ermittelt werden und Alarmobjekte, deren Ähnlichkeit einen vorgegebenen Alarmobjekt-Ähnlichkeitsschwellenwert übersteigt, als gleich angesehen und zu einem aggregierten Alarmobjekt zusammengefasst werden, dass die aggregierten Alarmobjekte der Alarmobjektgruppen jeweils paarweise miteinander verglichen werden, und dass diejenigen Alarmobjektpaare ermittelt werden, deren Ähnlichkeit am größten ist, indem die Häufigkeiten der einzelnen zugeordneten Alarmobjekte verglichen werden,
c) dass zunächst innerhalb der einzelnen Alarmobjektgruppen Alarmobjekte, deren Ähnlichkeit einen vorgegebenen Alarmobjekt-Ähnlichkeitsschwellenwert übersteigt, als gleich angesehen und zu einem aggregierten Alarmobjekt zusammengefasst werden, dass die aggregierten Alarmobjekte der einzelnen Alarmobjektgruppen Positionen innerhalb des jeweiligen Abschnitts der Alarmsequenz, den die jeweilige Alarmobjektgruppe umfasst, zugeordnet werden und dass mittels Sequenzalignment die Ähnlichkeiten der aggregierten Alarmobjekte der als ähnlich erkannten Alarmobjektgruppen ermittelt werden.

[0031] Gemäß einer vorteilhaften Ausführungsform eines erfindungsgemäßen Verfahrens kann auf besonders zuverlässige Weise sichergestellt werden, dass neu hinzugekommene Alarmobjekte bzw. Alarmobjektgruppen bei der Erstellung der Alarmobjektmuster berücksichtigt werden,

wenn das Zusammenfassen der Alarmobjektgruppen zu Alarmobjektmustern nach einer erstmaligen Erkennung neuerlich, insbesondere laufend, durchgeführt wird und die repräsentativen Alarmobjekte der einzelnen Alarmobjektmuster auf Grundlage der, in den neu hinzugekommenen, als ähnlich erkannten, Alarmobjektgruppen enthaltenen, Alarmobjekte, insbesondere mit einem erfindungsgemäßen Verfahren, aktualisiert werden,
wobei insbesondere vorgesehen ist, dass die bereits erstellten Alarmobjektmuster mit den neu erstellten Alarmobjektgruppen mit einem erfindungsgemäßen Verfahren zusammengefasst werden.

[0032] Eine besonders rasche und rechenleistungsschonende Vorgehensweise zur Klassifizierung des Angriffstyps auf dem neu hinzugekommen Alarmobjekte bzw. Alarmobjektgruppen basieren, kann bereitgestellt werden,
- wenn für neu erstellte Alarmobjektgruppen die Ähnlichkeit mit den bereits erstellten Alarmobjektmustern berechnet wird, wobei eine neue erstellte Alarmobjektgruppe als einem Alarmobjektmuster ähnlich erkannt wird, wenn die berechnete Ähnlichkeit zwischen der jeweiligen Alarmobjektgruppe und dem jeweiligen Alarmobjektmuster einen vorgegebenen Ähnlichkeitsschwellenwert übersteigt, und
- wenn diejenigen Alarmobjektmuster, denen die neu erstellten Alarmobjektgruppen als ähnlich erkannt wurden, auf Grundlage der, in den neu hinzugekommenen Alarmobjektgruppen enthaltenen, Alarmobjekte aktualisiert, insbesondere die jeweiligen Alarmobjektmuster mit den neu erstellten Alarmobjektgruppen mit einem erfindungsgemäßen Verfahren zusammengefasst, werden,
    wobei, im Fall, dass diejenige Alarmobjektgruppe, die als einem Alarmobjektmuster ähnlich erkannt wird, die gleichen Attribute aufweist, wie die Alarmobjektgruppen, auf denen das jeweilige Alarmobjektmuster basiert, die Attribute der repräsentativen Alarmobjekte des Alarmobjektmusters unverändert bleiben, und/oder
- wenn ein neues Alarmobjektmuster erstellt wird, wenn die Ähnlichkeit zwischen den neu erstellten Alarmobjektgruppen und den bereits erstellten Alarmobjektmustern den vorgegebenen Ähnlichkeitsschwellenwert nicht übersteigt.

[0033] Ein Programm zur Durchführung eines erfindungsgemäßen Verfahrens kann vorteilhafterweise auch auf einem Datenträger gespeichert sein.

[0034] Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der Beschreibung und den beiliegenden Zeichnungen.

[0035] Die Erfindung ist im Folgenden anhand von besonders vorteilhaften, aber nicht einschränkend zu verstehenden Ausführungsbeispielen in den Zeichnungen schematisch dargestellt und wird unter Bezugnahme auf die Zeichnungen beispielhaft beschrieben.

[0036] Im Folgenden zeigen:

[0037] Fig. 1 — ein Ausführungsbeispiel für das Zusammenfassen von Alarmobjekten zu Alarmobjektgruppen und das Zusammenfassen von Alarmobjektgruppen zu Alarmobjektmustern,

[0038] Fig. 2 — ein Ausführungsbeispiel für das Zusammenfassen von Alarmobjekten zu Alarmobjektgruppen basierend auf verschiedenen zeitlichen Abstandsschwellenwerten,

[0039] Fig. 3 — Ausführungsbeispiele für das Zusammenfassen von Alarmobjektgruppen zu Alarmobjektmustern,

[0040] Fig. 4 — ein erstes Ausführungsbeispiel eines erfindungsgemäßen Verfahrens mit einer Datenbank und zwei verschiedenen zeitlichen Abstandsschwellenwerten,

[0041] Fig. 5 — ein zweites Ausführungsbeispiel eines erfindungsgemäßen Verfahrens mit einer Datenbank und zwei verschiedenen zeitlichen Abstandsschwellenwerten,

[0042] Fig. 6, Fig. 7, Fig. 8 Beispiele für Alarmobjekte und Alarmobjektgruppen verschiedener Angriffserkennungssysteme,

[0043] Fig. 9, Fig. 10 Beispiele für repräsentative Alarmobjekte und Alarmobjektmuster,

[0044] Fig. 11, Fig. 13 weitere Beispiele für Alarmobjekte und Alarmobjektgruppen verschiedener Angriffserkennungssysteme,

[0045] Fig. 12, Fig. 14 weitere Beispiele für repräsentative Alarmobjekte und Alarmobjektmuster.

ALLGEMEINE VERFAHRENSBESCHREIBUNG

[0046] Fig. 1 erörtert die wichtigsten Konzepte der Erfindung: Der obere Teil von Fig. 1 stellt Alarmobjekte AO_1, ..., AO_{16} dar, die als Abfolgen von Ereignissen auf Zeitlinien auftreten. Die Abbildung enthält zwei Zeitachsen, um darzustellen, dass Alarmobjekte AO_1, ..., AO_{16} von verschiedenen Angriffserkennungssystemen S_A, S_B,... gesammelt werden können, die entweder in derselben Netzwerkinfrastruktur oder auch in getrennten Systemumgebungen eingesetzt werden. Eine weitere Möglichkeit besteht darin, dass Ereignisse aus historischen Alarmobjektprotokollen abgerufen und für die forensische Analyse von Angriffsmanifestationen verwendet werden.

[0047] Fig. 1 zeigt Alarmobjekte AO_1, ..., AO_{16} mit spezifischen Symbolen (Rechtecke, Kreise, Dreiecke, Balken), die einen bestimmten dem Alarmobjekt AO_1, ..., AO_{16} zugeordneten Typ repräsentieren, wobei ein Typ aufgrund eines oder mehrerer, insbesondere allen, übereinstimmenden Attributen und den Attributen zugehörige Werten, definiert ist, und insbesondere durch eine in dieser Erfindung beschriebenen Ähnlichkeitsmetrik bestimmt werden kann, wobei zwei Alarmobjekten dann der gleiche Typ zugeordnet wird, wenn sie eine ausreichend große Ähnlichkeit aufweisen, insbesondere eine Ähnlichkeit größer als ein bestimmter Schwellenwert.

[0048] Im Allgemeinen stellt jedes Alarmobjekt AO_1, ..., AO_{16} ein einzigartiges Ereignis dar, das nur zu einem bestimmten Zeitpunkt eintritt. Allerdings können Alarmobjekte AO_1, ..., AO_{16} desselben Typs, z.B. Alarmobjekte AO_1, ..., AO_{16}, die durch die Verletzung einer bestimmten vordefinierten Regel erzeugt werden, oder Alarmobjekte AO_1, ..., AO_{16}, die von denselben Angriffserkennungssystemen S_A, S_B,... gemeldet werden, mehrfach auftreten. Diese Alarmobjekte AO_1, ..., AO_{16} werden entsprechend mit dem gleichen Symbol gekennzeichnet. Alarmobjekte AO_1, ..., AO_{16}, die sich nur durch wenige zusätzliche, fehlende, oder veränderte Attribute unterscheiden, beispielsweise durch eines von mehreren abweichenden Attributen, werden beispielhaft zwar mit dem gleichen, aber gedrehten Symbol dargestellt. In oben gezeigter Grafik ist dies bei dem Dreieck, das die Alarmobjekte AO_2, AO_6, AO_8, AO_{12}, AO_{15} repräsentiert, sichtbar, dessen Spitze einige Male nach oben und einige Male nach unten zeigt.

[0049] Wie schon zuvor erwähnt, ist die Zuordnung von Alarmobjekten AO_1, ..., AO_{16} zu abstrakten Alarmobjektmustern P_1, ..., P_k, d.h., Mustern, die ein typisches Auftreten von einem oder mehreren Alarmobjekten AO_1, ..., AO_{16} repräsentativ beschreiben, nicht trivial.

[0050] In dem einfachen Beispiel in Fig. 1 ist zu erkennen, dass die Sequenz der Alarmobjekttypen Rechteck-Dreieck-Kreis manchmal mit dem mit der Spitze nach oben zeigenden Dreiecks und manchmal mit dem mit der Spitze des nach unten zeigenden Dreiecks vorkommt, insgesamt aber dreimal auftritt. Das Muster Kreis-Kreis-Dreieck tritt zweimal in den beiden Zeitlinien auf. Diese Gruppen sind für den Menschen intuitiv sichtbar, da diese Alarmobjekte nahe beieinander liegen und nicht durch andere Alarmobjekttypen unterbrochen werden. Da ein gemeinsames Auftreten von mehreren Alarmobjekten ein wesentlich genauerer Indikator für eine bestimmte auslösende Aktion ist als jeweils alle einzeln auftretenden Alarmobjekte alleine, ist es sinnvoll, Alarmobjekte solchen Alarmobjektgruppen G_1, ..., G_6 zuzuordnen. Der mittlere Teil von Fig. 1 zeigt Alarmobjektgruppen G_1, ..., G_6 auf der Grundlage ihrer jeweiligen zeitlichen Position auf den Zeitachsen.

[0051] Eine Gruppierung nach Alarmobjekttypen statt nach zeitlicher Nähe ist bei einem erfindungsgemäßen Verfahren zwar ebenfalls möglich, hätte aber unter Umständen einen Informationsverlust zur Folge, da Alarmobjekte AO_1, ..., AO_{16} unabhängig von ihrem Kontext, d.h. anderen

Alarmobjekten AO_1, ..., AO_{16}, die vermutlich von derselben auslösenden Aktion erzeugt werden, Alarmobjektgruppen G_1, ..., G_6 zugeordnet worden wären. Beispielsweise hätte eine Gruppierung aller Warnmeldungen des Typs Kreis die Tatsache vernachlässigt, dass dieser Typ sowohl in den Mustern Rechteck-Dreieck-Kreis sowie Kreis-Kreis-Dreieck auftritt, und wäre daher für sich allein genommen möglicherweise kein guter Indikator für eine bestimmte Angriffsausführung.

[0052] Die Reihenfolge, Häufigkeit und Attribute der Alarmobjekte AO_1, ..., AO_{16} innerhalb der Alarmobjektgruppen G_1, ..., G_6 ermöglichen die Berechnung von Ähnlichkeiten zwischen ihnen. Alarmobjektgruppen G_1, ..., G_6, die eine hohe Ähnlichkeit ergeben, stehen wahrscheinlich mit derselben Grundursache in Zusammenhang und sollten daher zu einer komprimierten Form zusammengefasst werden, die einen typischen Fall dieser Alarmobjektgruppe G_1, ..., G_6 widerspiegelt, was im Zusammenhang mit der Erfindung als ein Alarmobjektmuster P_1, ..., P_k bezeichnet wird.

[0053] Der untere Teil der Fig. 1 zeigt die Generierung von Alarmobjektmustern P_1, ..., P_k aus ähnlichen Alarmobjektgruppen G_1, ..., G_6. Dabei werden Ordnungen, Häufigkeiten und Attribute der Alarmobjektmuster P_1, ..., P_k so erstellt, dass alle zugeordneten Alarmobjektgruppen G_1, ..., G_6 so gut wie möglich repräsentiert werden.

[0054] Fig. 1 zeigt, dass dies durch die Zusammenführung der Alarmobjektgruppen G_1, G_3, G_6, die durch die Symbole Rechteck-Dreieck-Kreis repräsentierte Alarmobjekte umfassen, zum Alarmobjektmuster P_1 erreicht wird. Dabei wird ein repräsentatives Alarmobjekt RA_2, d.h. z.B. ein neuer Alarmobjekttyp, dargestellt aus zwei verbundenen Dreiecken, die sowohl nach oben als auch nach unten zeigen, erstellt wird. Dieses repräsentative Alarmobjekt RA_2 ist somit ein Mischtyp aus den bestehenden Dreieck-Alarmobjekttypen AO_2, AO_8, AO_{15}. Das könnte beispielsweise bedeuten, dass zwei verschiedene Attribute der ursprünglichen Alarmobjekte AO_2, AO_8, AO_{15} zu einer Liste zusammengefasst werden, worauf im Folgenden noch näher eingegangen wird.

[0055] Das zweite Alarmobjektmuster P_2 mit dem Alarmobjekttyp-Muster Kreis-Kreis-Dreieck wird aus den zwei identischen Alarmobjektgruppen G_2, G_4 gebildet und die repräsentativen Alarmobjekt RA_4, RA_5, RA_6 entsprechen daher den ursprünglichen Alarmobjekttypen der Alarmobjektgruppen G_2, G_4.

[0056] Wenn die Generierung von Alarmobjektmustern P_1, ..., P_k auf der Ähnlichkeit der Alarmobjekte AO_1, ..., AO_n und nicht auf Alarmobjektgruppen G_1, ..., G_m basieren würde und angenommen würde, dass das Dreieck mit der Spitze nach unten und das Dreieck mit der Spitze nach oben ähnliche Alarmobjekte AO_1, ..., AO_n repräsentieren, wären alle ihre Vorkommnisse durch den vorher genannten Mischtyp als repräsentatives Alarmobjekt RA ersetzt worden, und hätten somit die Genauigkeit des zweiten Alarmobjektmusters P_1, ..., P_k verringert. Dies legt nahe, dass die Bildung von Alarmobjektgruppen G_1, ..., G_m logisch zusammenhängender Alarmobjekte AO_1, ..., AO_n ein wesentlicher Vorteil bei der Generierung von Alarmobjektmustern P_1, ..., P_k ist.

[0057] Abschließend enthält des dritte Alarmobjektmuster P_3 ein einziges repräsentatives Alarmobjekt RA_7 (Balken), das nur einmal auftritt und das einzige Alarmobjekt in seiner Gruppe G_5 ist.

DETAILLIERTE VERFAHRENSBESCHREIBUNG

[0058] Als Datengrundlage für ein erfindungsgemäßes Verfahren wird eine Alarmobjektsequenz aus einem oder mehreren Angriffserkennungssystemen S_A, S_B genutzt, in der die einzelnen Alarmobjekte AO_1, ..., AO_n in der Abfolge ihres Auftretens, insbesondere versehen mit einem Zeitstempel, enthalten sind, wobei den einzelnen Alarmobjekten AO_1, ..., AO_n jeweils eine Anzahl von Attributen und den Attributen zugeordnete Werte, insbesondere eine Anzahl von Zahlen, Zeichenketten und/oder Objekten, zugeordnet sind, die den jeweils aufgetretenen anomalen Betriebszustand, der vom jeweiligen Angriffserkennungssystem S_A, S_B als einem Erkennungsfall entsprechend erkannt wurde, charakterisieren.

[0059] Der erste Schritt eines erfindungsgemäßen Verfahrens ist die Bildung von Alarmobjektgruppen G_1, ..., G_m aus diesen eingehenden Alarmobjekten AO_1, ..., AO_n. Dabei werden z.B. diejenigen Alarmobjekte AO_1, ..., AO_n zu einer Alarmobjektgruppe G_1, ..., G_m zusammengefasst, de-

ren Abstände zum jeweils nächsten Alarmobjekt AO in der Alarmobjektsequenz einen vorgegebenen zeitlichen Abstandsschwellenwert δ unterschreiten.

[0060] Fig. 2 verdeutlicht dieses Vorgehen, wobei jede Markierung an jedem Zeitstrahl eine Distanz von einer Zeiteinheit bedeutet. Wie in Fig. 2 zu sehen ist, führen kleinere zeitliche Abstandsschwellenwerte δ zur Bildung einer größeren Anzahl von Alarmobjektgruppen G. So werden bei einem zeitlichen Abstandsschwellenwert δ=0,5 Zeiteinheiten jeweils nur noch einzelne Alarmobjekte A zu einer Alarmobjektgruppe G zusammengefasst, während bei einem zeitlichen Abstandsschwellenwert δ=3,5 Zeiteinheiten jeweils am drei bzw. vier einzelne Alarmobjekte AO zu zwei Alarmobjektgruppen G zusammengefasst werden.

[0061] Eine manuelle Angabe eines bestimmten zeitlichen Abstandsschwellenwerts als maximal zulässiger zeitlichen Abstandsschwellenwert δ zwischen den Alarmobjekten AO_1, ..., AO_n ist nicht trivial, da ein hohes Maß an Wissen über die Interaktionen der Alarmobjekte AO_1, ..., AO_n und die erwarteten Strukturen der Alarmobjektsequenzen einfließen. Dazu kommt, dass unterschiedliche Alarmobjektmuster P_1, ..., P_k spezifische Einstellungen für den zeitlichen Abstandsschwellenwert δ erfordern können, die jedoch untereinander inkompatibel sind. Um dieses Problem zu lösen, kann die Alarmobjektgruppenbildung für mehrere zeitliche Abstandsschwellenwerte δ parallel durchgeführt werden. Dadurch erhöht sich die Wahrscheinlichkeit, dass für verschiedene Arten von Mustern von Alarmobjekten AO_1, ..., AO_n gültige und brauchbare Alarmobjektmustern P_1, ..., P_k gefunden werden.

[0062] Das Vergleichen und Zusammenfassen bzw. Aggregieren von Alarmobjektgruppen G_1, ..., G_n zu Alarmobjektmustern P_1, ..., P_n wird in Fig. 3 schematisch dargestellt. In Fig. 3 sind in drei Spalten jeweils drei Alarmobjektgruppen G_1, G_2, G_3; G_4, G_5, G_6; G_7, G_8, G_9 untereinander dargestellt, für die anhand einer vorgegebenen Ähnlichkeitsmetrik die Ähnlichkeit ermittelt werden soll, und die jeweils zu einer einzigen Alarmobjektgruppe G aggregiert werden sollen.

[0063] Die strichlierten und durchgezogenen Pfeile in Fig. 3 haben eine unterschiedliche Bedeutung: Die durchgezogenen Pfeile in Fig. 3 stellen dar, wie Alarmobjektgruppen G_1, G_2, G_3; G_4, G_5, G_6; G_7, G_8, G_9 miteinander aggregiert werden - an der Spitze des Pfeils steht also die jeweils aus den einzelnen Alarmobjektgruppen G_1, G_2, G_3; G_4, G_5, G_6; G_7, G_8, G_9 aggregierte Alarmobjektgruppe. Die strichlierten Pfeile in Fig. 3 stellen dar, dass eine einzelne Alarmobjektgruppe G_1, G_2, G_3; G_4, G_5, G_6; G_7, G_8, G_9 zu einer anderen Darstellungsform umgewandelt wird, und zwar immer in der Reihenfolge: Ursprüngliche Alarmobjektgruppe (links) -> Häufigkeitsbasierte Alarmobjektgruppe (Mitte) -> Sequenzalignmentbasierte Alarmobjektgruppe (rechts).

Insgesamt werden drei Möglichkeiten betrachtet:

[0064] Die linke Seite der Fig. 3 zeigt die erste Möglichkeit, wobei die Alarmobjekte AO der drei Alarmobjektgruppen G_1, G_2, G_3 miteinander verglichen werden. Insbesondere wird eine Ähnlichkeitsmetrik für Alarmobjekte AO festgelegt, um so das Auffinden von Paaren von Alarmobjekten AO über mehrere Alarmobjektgruppen G_1, G_2, G_3 hinweg zu ermöglichen, die eine hohe Ähnlichkeit erzielen. Dadurch ist es vorteilhafterweise nicht notwendig, vorauszusetzen, dass alle Alarmobjekte AO in der gleichen Reihenfolge in den einzelnen Alarmobjektgruppen G_1, G_2, G_3 auftreten.

[0065] Mit Hilfe der Ähnlichkeitsmetrik für Alarmobjekte AO werden dabei die Attribute aller Alarmobjekte AO verglichen, wobei idente oder ähnliche Attribute zu einer höheren Wahrscheinlichkeit zwischen Alarmobjekten AO beitragen, als unähnliche oder ungleiche Attribute. Die Gesamtähnlichkeit einer Alarmobjektgruppe G_1, G_2, G_3 wird dann als ein gewichtetes Mittel, insbesondere der Durchschnitt, aller Ähnlichkeiten der gefundenen Alarmobjekt-Paare berechnet.

[0066] Um Alarmobjektgruppen G_1, ..., G_m zu aggregieren, kann wiederum ein Auffinden von Paaren von zusammengehörigen Alarmobjekten AO_1, ..., AO_n verwendet werden, um diese dann einzeln zu Aggregieren und deren Gesamtheit der Alarmobjektgruppe zuzuordnen. Diese zweite Möglichkeit ist in der Mitte der Fig. 3 für die Alarmobjektgruppen G_4, G_5, G_6 schematisch dargestellt.

[0067] Besonders vorteilhaft können in diesem Zusammenhang beim Aggregieren der Alarmobjekte AO_1, ..., AO_n diejenigen Attribute, die in allen Alarmobjekten AO_1, ..., AO_n gleich sind, als einfache Attribute eingefügt werden. Weiters können besonders vorteilhaft, diejenigen Attribute, die wenige Ausprägungen, insbesondere mit einer Anzahl unterhalb eines vorgegebenen Schwellenwerts, über die Alarmobjekte AO_1, ..., AO_n hinweg annehmen, als Listen gespeichert werden.

[0068] Außerdem können vorteilhafterweise diejenigen Attribute, die viele Ausprägungen über die Alarmobjekte AO_1, ..., AO_n hinweg annehmen, insbesondere mit einer Anzahl über einen bestimmten Schwellenwert, als Platzhalter, die beliebige Werte annehmen können, gespeichert werden. Die Ähnlichkeitsmetrik der Alarmobjekte AO_1, ..., AO_n könnte dann die Attribute, die einen der in den Listen gespeicherten Werte annehmen, sowie diejenigen Attribute, die zu den Platzhaltern zugeordnet werden, positiv auf die Gesamtähnlichkeit auswirken lassen. Solch eine Zuordnung von Platzhaltern und Listen zu Attributen von Alarmobjekten wird im Folgenden als Aggregationsmethode für Alarmobjekte bezeichnet.

[0069] Der mittlere Teil der Fig. 3 zeigt eine besonders effiziente Methode zum Finden der Ähnlichkeit von Alarmobjektgruppen G_4, G_5, G_6 und Erstellen einer aggregierten Alarmobjektgruppe bzw. des Alarmobjektmusters P_2, unabhängig von der Position der Alarmobjekte AO_1, ..., AO_n in den jeweiligen Alarmobjektsequenzen. Dabei werden in der Mitte von Fig. 3 innerhalb jeder Alarmobjektgruppe G_4, G_5, G_6 zuerst die Häufigkeiten aller Alarmobjekte AO_1, ..., AO_n bestimmt, wobei ähnliche Alarmobjekte A, also Alarmobjekte A, deren Ähnlichkeit einen vorgegebenen Alarm-Ähnlichkeitsschwellenwert für die minimale Ähnlichkeit für Alarmobjekte AO überschreiten, als gleich angesehen werden, und jede Menge an Alarmobjekten AO wird im des Alarmobjektmusters P_2 bzw. in der aggregierten Alarmobjektgruppe durch ein repräsentatives Alarmobjekt RA_7, RA_8, RA_9 dargestellt wird, das sich als Aggregation aller ähnlichen Alarmobjekte AO ergibt.

[0070] Dann wird wie zuvor eine Zuordnung zwischen den repräsentativen Alarmobjekten RA_7, RA_8, RA_9 über die Alarmobjektgruppen G_1, ..., G_m hinweg durchgeführt, wobei sich in diesem Fall die Anzahl der notwendigen Vergleiche von der Gesamtheit der Alarmobjekte AO_1, ..., AO_n auf die repräsentativen Alarmobjekte RA_7, RA_8, RA_9 reduziert hat.

[0071] Die Ähnlichkeit der Alarmobjektgruppen G_1, ..., G_m kann nun einerseits bestimmt werden, indem die Häufigkeiten der zugeordneten repräsentativen Alarmobjekte RA_7, RA_8, RA_9 verglichen wird. Beispielsweise kann das Verhältnis der Häufigkeiten bestimmt werden, sodass übereinstimmende Häufigkeiten einen positiven Einfluss auf die Ähnlichkeit haben, geringe Abweichungen einen negativen Einfluss auf die Ähnlichkeit haben, und starke Abweichungen einen stark negativen Einfluss auf die Ähnlichkeit haben.

[0072] Ein Zusammenfassen bzw. eine Aggregation der Alarmobjektgruppen G_1, ..., G_m zu einem Alarmobjektmuster P_2 ist anschließend möglich, indem Grenzen für die jeweiligen Häufigkeiten der vorkommenden repräsentativen Alarmobjekte RA_7, RA_8, RA_9 festgelegt werden, sodass alle Alarmobjektgruppen G_1, ..., G_m diesen Häufigkeitsintervallen entsprechen, das heißt, dass für jedes der repräsentativen Alarmobjekte RA_7, RA_8, RA_9 die minimale und maximale Häufigkeit der den repräsentativen Alarmobjekten zugehörigen Alarmobjekte AO_1, ..., AO_n bestimmt und als minimale und maximale Grenzen für die Häufigkeiten der repräsentativen Alarmobjekte RA_7, RA_8, RA9 im Alarmobjektmuster festgelegt werden. Die zugehörigen Alarmobjekte AO_1, ..., AO_n zu diesen Häufigkeitsverteilungen werden wiederum durch eine Aggregation der repräsentativen Alarmobjekte RA_7, RA_8, RA_9 der Alarmobjektgruppen G_1, ..., G_m erzeugt.

[0073] Die rechte Seite der Fig. 3 zeigt eine besonders effiziente Methode zum Finden der Ähnlichkeit der Alarmobjektgruppen G_7, G_8, G_9 und Erstellen einer aggregierten Alarmobjektgruppe bzw. des Alarmobjektmusters P_3 basierend auf den Positionen der Alarmobjekte AO_1, ..., A_n in den jeweiligen Alarmobjektsequenzen. Dabei werden die repräsentativen Alarmobjekte RA_7, RA_8, RA_9, die im Zuge der vorherigen Methode erstellt wurden, den Positionen der ursprünglichen Alarmobjekte AO_1, ..., AO_n in den jeweiligen Alarmobjektsequenzen der Alarmobjektgruppen G_7, G_8, G_9 zugeordnet. Dann ist es mithilfe von bekannten Methoden aus dem Sequenzalignment (siehe z.B. Gonzalo Navarro. 2001. A guided tour to approximate string matching. ACM computing surveys (CSUR) 33, 1 (2001), 31-88), die die notwendigen Änderungsoperationen zählen,

um die jeweiligen Alarmobjektsequenzen in Übereinstimmung zu bringen, möglich, die Ähnlichkeit der Alarmobjektgruppen G_7, G_8, G_9 zu bestimmen. Ebenso können diese Methoden, insbesondere für das Feststellen einer längsten gemeinsamen und möglicherweise unterbrochenen Alarmobjektkette, die in allen Alarmobjektgruppen G_7, G_8, G_9 vorhanden ist, verwendet werden, um das Alarmobjektmuster P_3 bzw. die aggregierte Alarmobjektgruppe zu erstellen.

[0074] Anhand der Fig. 4 wird beispielhaft ein erstes Ausführungsbeispiel eines erfindungsgemäßen Verfahrens mit zwei zeitlichen Abstandsschwellenwerten δ_{large} und δ_{small} und einer Datenbank D erläutert. In der Datenbank D werden die erstellten Alarmobjektgruppen G_1, ..., G_4 hinterlegt und Alarmobjektmuster P_1, P_2 werden auf Grundlage der in der Datenbank D hinterlegten Alarmobjektgruppen G_1, ..., G_4 erstellt. Diese Alarmobjektmuster P_1, P_2, sowie die Zugehörigkeit der einzelnen Alarmobjektgruppen G1, ..., G4 zu den einzelnen Alarmobjektmustern P_1, P_2 werden ebenfalls in der Datenbank D hinterlegt. Aus Gründen der Übersichtlichkeit sind in Fig. 5 die einzelnen Alarmobjekte AO_1, ..., AO_n der Alarmgruppen G_1, ..., G_3; G'_1, ..., G'_6 nicht mit Bezugszeichen gekennzeichnet.

[0075] Das erste Ausführungsbeispiel in Fig. 4 dargestellt und befasst sich mit dem Finden von Alarmobjektmustern P_1, P_2 und der Wiedererkennung dieser Alarmobjektmuster P_1, P_2 auf verschiedenen Angriffserkennungssystemen S_A, S_B. Der untere Teil der Fig. 4 zeigt das Auftreten von Alarmobjekten AO_1, ..., AO_n in Form von Alarmobjektsequenzen, die von den Angriffserkennungssystemen S_A, S_B erzeugt werden. In den Alarmobjektsequenzen sind die einzelnen Alarmobjekte AO_1, ..., AO_n in der Abfolge ihres Auftretens, z.B. versehen mit einem Zeitstempel enthalten, die von den beiden Angriffserkennungssystemen S_A, S_B erstellt werden. Der mittlere Teil der Fig. 4 beinhaltet die erstellten Alarmobjektmuster P_1, P_2.

[0076] Der obere Teil der Fig. 4 zeigt eine Datenbank D, in der im Ausführungsbeispiel alle erstellten Alarmobjektgruppen G_1, ..., G_4, sowie deren Zuordnungen zu den erstellten Alarmobjektmustern P_1, P_2 gespeichert werden. Das bedeutet, dass jede Alarmobjektgruppe G_1, ..., G_4 von Alarmobjekten AO_1, ..., AO_n, die erkannt wurde, in dieser Datenbank D dauerhaft gespeichert wird, und dass zu jeder dieser Alarmobjektgruppen G_1, ..., G_4 eine Referenz zum zugehörigen Alarmobjektmuster P_1, P_2 gespeichert wird, z.B. in Form einer Liste für jedes Alarmobjektmuster P_1, P_2 mit Referenzen zu den zugehörigen Alarmobjektgruppen G_1, ..., G_4. Es ist somit möglich, alle einem Alarmobjektmuster P1, P2 zugehörigen Alarmobjektgruppen G_1, ..., G_4 zu erhalten, indem über alle Referenzen auf Alarmobjektgruppen G_1, ..., G_4, die in der für diesen Alarmobjektmuster P_1, P_2 gespeicherten Liste vorhanden sind, iteriert wird.

[0077] Die Datenbank D stellt somit vorteilhafterweise sicher, dass Alarmobjektmuster P_1, P_2 quasi als repräsentative aggregierte Alarmobjektgruppe für alle in der Datenbank D gespeicherten Alarmobjektgruppen G_1, ..., G_4 erzeugt werden. Zwar funktioniert ein erfindungsgemäßes Verfahren auch ohne eine derartige Datenbank D ausreichend zuverlässig. Eine derartige Datenbank D verhindert allerdings vorteilhafterweise, dass die bestehenden Alarmobjektmuster P_1, P_2 immer weiter verändert werden, sobald neue Alarmobjektgruppen G zugeordnet werden, was zu einer Übergeneralisierung führen könnte. Da übergeneralisierte Alarmobjektmuster P_1, P_2 umso mehr Zuordnungen von neu erstellten Alarmobjektgruppen G erhalten, könnte sich dieser Effekt über die Zeit sogar verstärken, was durch eine Datenbank D zuverlässig verhindert wird.

[0078] Das Erstellen einer Datenbank könnte unter Umständen mit einer erhöhten Komplexität des Verfahrensablaufs, einer Erhöhung des Speicherbedarfs, da zu jedem Alarmobjektmuster P_1, ..., P_k eine Menge an Alarmobjektgruppen G_1, ..., G_m gespeichert werden, und einer Erhöhung der Laufzeit, da bei jeder Neuerstellung eines Alarmobjektmusters P_1, ..., P_k mehrere Alarmobjektgruppen G_1, ..., G_m aggregiert werden, einhergehen. Dies könnte vor allem im Betrieb in Echtzeit zu Problemen führen, wenn sich die Anzahl der Alarmobjektgruppen G_1, ..., G_m stetig erhöht und somit bei längerem Betrieb aufgrund einer zu hohen Rechenzeit, die durch die Aggregation der den Alarmobjektmustern P_1, ..., P_k zugehörigen Alarmobjektgruppen G_1, ..., G_m verursacht werden könnte, neue Alarmobjekte AO_1, ..., AO_n nicht mehr ohne große Verzögerung prozessiert werden würden.

[0079] Daher können bei einem erfindungsgemäßen Verfahren optional zur Vermeidung dieser

Probleme drei verschiedene Strategien zur Speicherung von Listen der zu Alarmobjektmustern P_1, ..., P_k zugehörigen Alarmobjektgruppen G_1, ..., G_m angewendet werden, die je nach Anwendungsfall ausgewählt werden können:

[0080] So kann die Zugehörigkeit der einzelnen Alarmobjektgruppen G_1, ..., G_m zu den einzelnen Alarmobjektmustern P_1, ..., P_k in Form von Listen umfassend die einem jeweiligen Alarmobjektmuster P_1, ..., P_k zugeordneten Alarmobjektgruppen G_1, ..., G_m in der Datenbank D hinterlegt werden. Dabei kann es sich um einen oder mehrere der folgenden Listentypen handeln:

[0081] • Unbeschränkte Listen: Diese Strategie impliziert, dass die Zahl der Listeneinträge unbegrenzt anwachsen kann. Eine solche Strategie ist nützlich für forensische Analysen, bei denen keine Prozessierung in Echtzeit notwendig ist und die Gesamtzahl der Alarmobjektgruppen G_1, ..., G_m begrenzt und klein genug ist, um alle Alarmobjektgruppen G_1, ..., G_m zu speichern.

[0082] • Linear befüllbare Listen: Bei dieser Strategie ist die Größe der Listen auf einen Fixwert begrenzt. Sobald die Größe einer Liste diesen Wert erreicht, führt das Hinzufügen einer neuen Alarmobjektgruppe G dazu, dass die älteste Alarmobjektgruppe in der Liste G_1, ..., G_m entfernt wird, womit sich die Listengröße nicht weiter ändert.

[0083] • Logarithmisch befüllbare Listen: Zuerst wird die Liste bis zu ihrer maximalen Größe wie bei einer linear befüllbaren Liste gefüllt. Dann ersetzt jede neu hinzugefügte Alarmobjektgruppe G_m die Alarmobjektgruppe G_m an der letzten Position mit einer Wahrscheinlichkeit von 50%, verschiebt die Alarmobjektgruppe G_m an der letzten Position mit einer Wahrscheinlichkeit von 25% um eine Position in Richtung der Alarmobjektgruppe G_1 an ersten Position und überschreibt somit die Alarmobjektgruppe G_{m-1} an der vorletzten Position, verschiebt die beiden letzten Alarmobjektgruppen mit einer Wahrscheinlichkeit von 12,5% gemeinsam um eine Position in Richtung der ersten Position und überschreibt somit die Alarmobjektgruppe G_{m-2} an der vorvorletzten Position, usw. Dadurch wird sichergestellt, dass Alarmobjektgruppen G_1, ..., G_m, die in den ersten Positionen der Liste gespeichert sind, länger in den Listen gespeichert bleiben und somit die Gesamtheit der in der Liste gespeicherten Alarmobjektgruppen G_1, ..., G_m eine vielfältigere und repräsentativere Menge darstellen. Diese Strategie ist daher besonders nützlich, wenn Alarmobjektgruppen G_1, ..., G_m über lange Zeitintervalle auftreten, z.B. wenn sie aus verschiedenen Systemumgebungen gesammelt werden.

[0084] In Fig. 4 werden jedem der horizontal voneinander getrennten Blöcke werden zwei Abschnitte angezeigt, einer für einen großen zeitlichen Abstandsschwellenwerten δ_{large} (oben) und einer für einen kleinen zeitlichen Abstandsschwellenwerten δ_{small} (unten). Wie in der Fig. 4 zu sehen ist, wird die Anzahl der gebildeten Alarmobjektgruppen durch den zeitlichen Abstandsschwellenwerten δ beeinflusst, d.h. für das Angriffserkennungssystem S_A werden zwei Alarmobjektgruppen G_1, G_2 für einen großen zeitlichen Abstandsschwellenwerten δ_{large} und vier Alarmobjektgruppen G'_1, ..., G'_4 für einen kleinen zeitlichen Abstandsschwellenwerten δ_{small} gebildet.

[0085] Der Einfachheit halber wird im Folgenden nur auf die Alarmobjektgruppen P_1, P_2, die für den großen zeitlichen Abstandsschwellenwerten δ_{large} gebildet werden, beginnend mit der ersten Alarmobjektgruppe P_1, die Alarmobjekte AO_1, ..., AO_6 umfasst, die durch ein sich zweimal wiederholendes Muster der Symbole Rechteck-Dreieck-Kreis repräsentiert werden.

[0086] Da am Beginn des Ablaufs eines erfindungsgemäßen Verfahrens zunächst keine Alarmobjektmuster P existieren, wird die Alarmobjektgruppe G1 in die Datenbank D aufgenommen und gleichzeitig als neues Alarmobjektmuster hinzugefügt, indem sie kopiert wird, wie in Schritt (1) angegeben in Fig. 4. Da zu diesem Zeitpunkt nur diese Alarmobjektgruppe G_1 in der Datenbank D existiert, ist der Alarmobjektmuster ident mit der ursprünglichen Alarmobjektgruppe G_1. Erst danach findet die Generierung eines Alarmobjektmusters P_1 aus mehreren Alarmobjektgruppen G_1, G_2 der Datenbank D statt, wie in Schritt (2) angegeben.

[0087] Die zweite Alarmobjektgruppe G_2, die vom Angriffserkennungssystem S_A unter Verwendung des großen zeitlichen Abstandsschwellenwerten δ_{large} identifiziert wurde, beinhaltet die glei-

che Abfolge an Alarmobjekten wie die erste Alarmobjektgruppe G_1. Schritt (3) zeigt, dass die Ähnlichkeit zwischen der zweiten Alarmobjektgruppe G_2 und dem Alarmobjektmuster P_1 berechnet wird.

[0088] Da es nur ein Alarmobjektmuster P_1 gibt und angenommen wird, dass die erreichte Ähnlichkeit mit der zweiten Alarmobjektgruppe größer als ein vordefinierter Alarmobjektgruppen-Ähnlichkeitsschwellenwert t ist, wird die zweite Alarmobjektgruppe G_2 der Datenbank D hinzugefügt, die die Alarmobjektgruppen G_1, G_2 speichert, die dem Alarmobjektmuster P_1 zugeordnet sind, wie in Schritt (4) angegeben.

[0089] Das Hinzufügen löst eine Neuerstellung des Alarmobjektmusters P_1 aus, wie in Schritt (5) angegeben. Die Neuerstellung des Alarmobjektmusters P_1 ist vorteilhaft, damit das Alarmobjektmuster P_1 stets einer typischen Repräsentation aller ihm zugeordneten Alarmobjektgruppen G_1, G_2, die in der Datenbank D gespeichert sind, entspricht, und somit auch den in der neu zugeordneten Alarmobjektgruppe G_2 enthaltenen Strukturen von Alarmobjekten AO_1, ..., AO_6 oder Abfolgen von Alarmobjekten ausreichend entspricht. Unter der Annahme, dass alle Alarmobjekte AO_1, ..., AO_6 in der ersten und zweiten Alarmobjektgruppe G_1, G_2 die gleichen Attribute haben, bleibt das neuerstellte Alarmobjektmuster P_1 unverändert.

[0090] Nun tritt eine dritte Alarmobjektgruppe G_3 im Angriffserkennungssystem S_B zu einem Zeitpunkt auf, der nach der Erstellung des Alarmobjektmusters P_1 von Angriffserkennungssystem S_A generiert wurde. Wie zuvor wird für die dritte Alarmobjektgruppe G_3 die Ähnlichkeit zu allen bisher vorhandenen Alarmobjektmustern, in Fig.4 ist dies nur das Alarmobjektmuster P_1, berechnet, wie in Schritt (6) gezeigt.

[0091] In diesem Fall stimmen nur die ersten vier Alarmobjekte AO_1, ..., AO_4 der sechs Alarmobjekte der Alarmobjektgruppe G_3 überein, was bedeutet, dass die Ähnlichkeit geringer ist als die zuvor berechnete Ähnlichkeit der zweiten Alarmobjektgruppe G_2 zum Alarmobjektmuster P_1. Ein Grund dafür könnten systemspezifische Attributwerte in Warnmeldungen oder Variationen der Angriffsausführung sein, die die Alarmobjekte auf Angriffserkennungssystem S_B entsprechend abändern. Unter der Annahme, dass die Ähnlichkeit ausreichend hoch ist, d.h. über dem vorgegebenen Alarmobjektgruppen-Ähnlichkeitsschwellenwert t liegt, kann dies als Erkennung einer Ausführung desselben Angriffs auf Angriffserkennungssystem S_B interpretiert werden.

[0092] Andernfalls wird ein neues Alarmobjektmuster P basierend der dritten Alarmobjektgruppe G_3 generiert. In jedem Fall wird die Alarmobjektgruppe G_3 der Datenbank D hinzugefügt, wie in Schritt (7) angegeben.

[0093] Eine Neugenerierung des Alarmobjektmusters bzw. Generierung eines weiteren Alarmobjektmusters ist in der Grafik nicht dargestellt, da sich das zweite Ausführungsbeispiel ausführlicher mit diesem Fall befasst.

[0094] Die Vorgehensweise für diejenigen Alarmobjektgruppen G'_1, ..., G'_4, die für den kleinen zeitlichen Abstandsschwellenwert δ_{small} identifiziert wurden, ist analog, aber aus Übersichtsgründen nicht in Fig. 4 eingezeichnet. Wie in der rechten Seite der Fig. 4 dargestellt, werden die vier auf Angriffserkennungssystem SA identifizierten Alarmobjektgruppen G'_1, ..., G'_4 iterativ, d.h. aufeinanderfolgend, zur Datenbank D hinzugefügt und alle zu einem einzigen Alarmobjektmuster P_2 zusammengeführt. Auf Angriffserkennungssystem S_B werden für den kleinen zeitlichen Abstandsschwellenwert δ_{small} zwei Alarmobjektgruppen G'_5, G'_6 identifiziert, von denen die Alarmobjektgruppen G'_5 die gleiche Alarmobjektsequenz wie das Alarmobjektmuster P_2 umfasst und daher ähnlich genug ist, um eine erfolgreiche Erkennung des dem Alarmobjektmuster P_2 zugeordneten Angriffstyp zu ergeben, während die andere Alarmobjektgruppen G'_6 nur eines von drei Alarmobjekten gemeinsam mit dem Alarmobjektmuster P_2 hat und daher nicht ähnlich genug ist, um als auf demjenigen Angriffstyp beruhend erkannt zu werden, der dem Alarmobjektmuster P_2 zugeordnet ist.

[0095] Das zweite Ausführungsbeispiel ist in Fig. 5 schematisch dargestellt und konzentriert sich auf die Zusammenlegung von Alarmobjektgruppen, die auf verschiedenen Angriffserkennungssystem S_A, S_B identifiziert wurden. Die in Fig. 5 markierten Schritte konzentrieren sich der Ein-

fachheit halber nur auf die Ergebnisse des kleinen zeitlichen Abstandsschwellenwerts δ_{small}. Aus Gründen der Übersichtlichkeit sind in Fig. 5 die einzelnen Alarmobjekte AO_1, ..., AO_n der Alarmgruppen G'_1, ..., G'_6 nicht mit Bezugszeichen gekennzeichnet.

[0096] Ähnlich wie im ersten Ausführungsbeispiel deuten die Schritte (1) und (2) auf die Generierung eines Alarmobjektmusters P_1 aus der ersten Alarmobjektgruppe G'_1 auf Angriffserkennungssystem S_A hin, wobei die Alarmobjektgruppe G'_1 zuerst der Datenbank D hinzugefügt wird und erst dann das Alarmobjektmuster P_1 erzeugt wird.

[0097] In diesem zweiten Ausführungsbeispiel unterscheidet sich jedoch die zweite Alarmobjektgruppe G'_2 von Angriffserkennungssystem S_A im zweiten und vierten Alarmobjekt von Alarmobjektgruppe G'_1, was dadurch angedeutet ist, dass die Spitzen der Dreiecke in unterschiedliche Richtungen zeigen. Es wird angenommen, dass die Alarmobjektgruppe G'_2 dennoch eine ausreichend hohe Ähnlichkeit bei der Prüfung in Schritt (3) ergibt und daher in Schritt (4) zur Datenbank D hinzugefügt und dem Alarmobjektmuster P_1 zugeordnet wird. Dies wiederum führt zur Neuerzeugung des Alarmobjektmusters P_1, wobei die erste als auch die zweite Alarmobjektgruppe G'_1, G'_2 aggregiert bzw. zusammengefasst werden. Das daraus resultierende Alarmobjektmuster P_1 ist eine Verschmelzung dieser Alarmobjektgruppen G'_1, G'_2, in der Art, dass der zweite und vierte Alarmobjekt ein Mischtyp aus den jeweiligen zweiten und vierten Alarmobjekten der ersten und zweiten Alarmobjektgruppe G'_1, G'_2 von Angriffserkennungssystem S_A darstellt.

[0098] Anders als im ersten Ausführungsbeispiel, wo es darum geht, dasselbe Alarmobjektmuster auf einem anderen System zu erkennen, werden jetzt auch die Alarmobjektgruppen von Angriffserkennungssystem S_B miteinbezogenen, um einen systemübergreifendes Alarmobjektmuster zu generieren.

[0099] Auf Angriffserkennungssystem S_B wurden für den kleinen zeitlichen Abstandsschwellenwert δ_{small} weitere vier Alarmobjektgruppen G'_3, ..., G'_6 identifiziert, und unter der Annahme, dass alle ähnlich genug zu dem Alarmobjektmuster P_1 sind, werden alle zur Datenbank D hinzugefügt und dem Alarmobjektmuster P_1 zugeordnet. Bei der Generierung des Alarmobjektmusters P_1 werden also die sechs Alarmobjektgruppen G'_1, ..., G'_6 zusammengefasst bzw. aggregiert.

[00100] In jeder Alarmobjektgruppe G'_1, ..., G'_6 sind das erste und das dritte Alarmobjekt vom gleichen Typ Kreis, welcher im resultierenden Alarmobjektmuster als repräsentatives Alarmobjekt RA_1 bzw. RA_3 beibehalten wird. In drei der Alarmobjektgruppen ist das zweite Alarmobjekt vom Typ Dreieck mit der Spitze nach oben, in den anderen drei ist es der Typ Dreieck mit der Spitze nach unten. Dementsprechend wird das zweite repräsentative Alarmobjekt RA_2 im Alarmobjektmuster P_1 in einem kombinierten Alarmobjekttyp, der aus zwei Dreiecken besteht, die jeweils mit der Spitze nach oben und unten zeigen, zusammengeführt, was im zweiten Ausführungsbeispiel bedeutet, dass ein Attribut des Alarmobjekts durch eine Liste mit zwei verschiedenen Werten dargestellt wird. Dadurch wird sichergestellt, dass das jeweilige Attribut jeder Alarmobjektgruppe G'_1, ..., G'_6 mit dem Attribut im Alarmobjektmuster P_1 übereinstimmt.

[00101] Das vierte Alarmobjekt hingegen ist diverser, da ein Alarmobjekttyp mit einem Dreieck, das in jede der vier möglichen Richtungen zeigt, in mindestens einer Alarmobjektgruppe G'_1, ..., G'_6 an dieser Position vorkommt. Dementsprechend ersetzt die Aggregationsmethode für Alarmobjekte das entsprechende Attribut des jeweiligen Alarmobjekts im Alarmobjektmuster P_1 durch ein repräsentatives Alarmobjekt RA_4 in Form eines Platzhalters, der durch den Alarmobjekttyp Stern gekennzeichnet ist. Beispielsweise könnte in dem betroffenen Attribut ein Zähler stehen, der sich bei jeder Ausführung ändert, und deshalb als variabel und nicht spezifisch für das Alarmobjekt oder Angriff gelten sollte. Da der Wert durch einen Platzhalter ersetzt wird, stimmen nicht nur die Alarmobjekte aller Alarmobjektgruppen G'_1, ..., G'_6 überein, sondern auch jeder Wert, der für dieses Attribut auftreten könnte.

[00102] Das zweite Alarmobjektmuster P_2, das basierend auf den Alarmobjektgruppen G_1, ..., G_3 der Angriffserkennungssystem S_A, S_B generiert wurde, die unter Verwendung des großen zeitlichen Abstandsschwellenwerts δ_{large} gebildet wurden, zeigt, dass die Abfolge der zusammengeführten Alarmobjekte vom ersten Alarmobjektmuster P1 abweicht, z.B. treten die Alarmobjektty-

pen Dreieck mit der Spitze nach oben sowie Dreieck mit der Spitze nach unten anstelle des kombinierten Alarmobjekttyps, der zwei Dreiecke beinhaltet, auf.

[00103] Dies legt nahe, dass es vorteilhaft ist, verschiedene zeitlichen Abstandsschwellenwerte δ gleichzeitig zu berücksichtigen, da jedes der erstellten Alarmobjektmuster P die bestmögliche Wiedererkennung ermöglichen könnte, je nachdem, welche Alarmobjekte AO bei einer erneuten Ausführung des Angriffs erstellt werden würden.

[00104] Im Folgenden wird dieses zweite Ausführungsbeispiel der Erfindung im Detail diskutiert. Im Gegensatz zur Fig. 5 werden aus Gründen der Vollständigkeit drei anstatt zwei zeitlichen Abstandsschwellenwerte δ_{large}, δ_{small} verwendet. Der dritte zeitlichen Abstandsschwellenwert δ_3 ist kleiner als beide in Fig. 5 dargestellten zeitlichen Abstandsschwellenwerte δ_{large}, δ_{small} und soll den Grenzfall verdeutlichen, bei dem aufgrund eines sehr kleinen zeitlichen Abstandsschwellenwertes ö jedes Alarmobjekt AO_1, ..., AO_n für sich eine eigene Alarmobjektgruppe G_1, ..., G_n bildet. Die beiden anderen zeitlichen Abstandsschwellenwerte δ_{large}, δ_{small} im Beispiel entsprechen genau den zeitlichen Abstandsschwellenwerten δ_{large}, δ_{small} der Fig. 5.

DETAILLIERTER VERFAHRENSABLAUF ANHAND DES ZWEITEN AUSFÜHRUNGSBEISPIELS

[00105] Im folgenden Ausführungsbeispiel werden Alarmobjekte AO_1, ..., AO_n als zeitliche Ereignisse mit verschiedenen semi-strukturierten Attributen betrachtet. Beispielhaft werden zwei Alarmobjekttypen verwendet, die sich stark in den jeweils vorhandenen Attributen unterscheiden.

[00106] Alarmobjekttyp 1 (dargestellt durch das Symbol Kreis) besitzt die Attribute A, B, und C, Alarmobjekttyp 2 (dargestellt durch das Symbol Dreieck) besitzt die Attribute X, Y, und Z. Jedes Attribut kann einen bestimmten Wert annehmen, zum Beispiel, X=x. Es ist möglich, dass komplexe Werte, wie zum Beispiel Listen oder weitere semi-strukturierte Objekte mit weiteren Attributen, angenommen werden. Im folgenden Beispiel werden jedoch nur einfache Werte verwendet. Insbesondere werden für die Attribute A, B, C, X, und Y, jeweils die Werte a, b, c, x, und y verwendet. Das Attribut Z kann eines von vier verschiedenen Werten einnehmen, diese sind z1, z2, z3, und z4 (siehe Tabelle 1).

[00107] Tabelle 1: Alarmobjekte AO_1, ..., AO_8 des Angriffserkennungssystems S_A:

Alarmobjekt-ID	**Zeitschritt**	**Attribut 1**	**Attribut 2**	**Attribut 3**
1	0	A=a	B=b	C=c
2	3	X=x	Y=y	Z=z1
3	6	A=a	B=b	C=c
4	9	X=x	Y=y	Z=z1
5	31	A=a	B=b	C=c
6	34	X=x	Y=y	Z=z3
7	37	A=a	B=b	C=c
8	40	X=x	Y=y	Z=z2

[00108] In Fig. 6 sind die Alarmobjekte AO_1, ..., AO_8 einer Alarmobjektsequenz des Angriffserkennungssystems SA visuell dargestellt (zeitliche Abstände sind nicht maßstabsgetreu).

[00109] Wobei die folgende Zuordnung von Symbolen und Alarmobjekt-Typen gewählt wurde:

- Alarmobjekttyp 1 (Attribute A=a, B=b, und C=c): Kreis
- Alarmobjekttyp 2 (Attribute X=x, Y=y, und Z=z1): Dreieck mit Spitze nach oben
- Alarmobjekttyp 2 (Attribute X=x, Y=y, und Z=z2): Dreieck mit Spitze nach rechts
- Alarmobjekttyp 2 (Attribute X=x, Y=y, und Z=z3): Dreieck mit Spitze nach unten
- Alarmobjekttyp 2 (Attribute X=x, Y=y, und Z=z4): Dreieck mit Spitze nach links

[00110] Tabelle 2: Alarmobjekte AO_9, ..., AO_{24} des Angriffserkennungssystems S_B:

Alarmobjekt-ID	Zeitschritt	Attribut 1	Attribut 2	Attribut 3
9	110	A=a	B=b	C=c
10	113	X=x	Y=y	Z=z1
11	116	A=a	B=b	C=c
12	119	X=x	Y=y	Z=z1
13	142	A=a	B=b	C=c
14	145	X=x	Y=y	Z=z3
15	148	A=a	B=b	C=c
16	151	X=x	Y=y	Z=z4
17	214	A=a	B=b	C=c
18	217	X=x	Y=y	Z=z1
19	220	A=a	B=b	C=c
20	223	X=x	Y=y	Z=z1
21	246	A=a	B=b	C=c
22	249	X=x	Y=y	Z=z3
23	252	A=a	B=b	C=c
24	255	X=x	Y=y	Z=z3

[00111] In Fig. 7 sind die Alarmobjekte AO_9, ..., AO_{24} (siehe Tabelle 2) einer Alarmobjektsequenz des Angriffserkennungssystems SB visuell dargestellt (zeitliche Abstände sind nicht maßstabsgetreu).

[00112] Zu beachten ist, dass die auftretenden Alarmobjekte AO_9, ..., AO_{24} wiederholende Abfolgen bzw. Muster bilden. Insbesondere wechseln sich der Alarmobjekttyp 1 und der Alarmobjekttyp 2 jeweils ab. Weiters häufen sich die Alarmobjekte an bestimmten Zeitpunkten: Jeweils vier Alarmobjekte treten im Abstand von 3 Sekunden auf und formen Alarmobjektgruppen (zum Beispiel Alarmobjekte AO_9-AO_{12} auf Angriffserkennungssystem S_B). Jeweils zwei dieser Alarmobjektgruppen treten im Abstand von 22 Sekunden auf (zum Beispiel Alarmobjekte AO_9-AO_{12} und Alarmobjekte AO_{13}-AO_{16}). In Angriffserkennungssystem SA tritt nur ein solches Paar auf (Alarmobjekte AO_1-AO_4 und Alarmobjekte AO_5-AO_8), in Angriffserkennungssystem SB treten zwei dieser Paare im Abstand von 63 Sekunden auf.

[00113] Im Folgenden werden die Zeitspannen 1 Sekunde, 10 Sekunden (entspricht dem kleinen zeitlichen Abstandsschwellenwert δ_{small} in Abb. Fig. 5), und 50 Sekunden (entspricht dem großen zeitlichen Abstandsschwellenwert δ_{large} in Fig. 5) als beispielhafte Wahl für den zeitlichen Abstandsschwellenwert δ_l betrachtet. Weiters wird ein Alarmobjektgruppen-Ähnlichkeitsschwellenwert t=0,5 als Mindestähnlichkeit für Alarmobjektgruppen G gewählt und eine Maximalgröße von 2 Einträgen für aggregierte Listen festgelegt.

[00114] Wird eine Zeitspanne von 1 Sekunde gewählt, so bildet jedes Alarmobjekt AO für sich eine Alarmobjektgruppe G, da zwischen keinen zwei Alarmobjekten AO eine kleinere zeitliche Distanz kleiner als 1 Sekunde besteht. Fig. 8 zeigt diese Alarmobjektgruppen G und die zugehörigen Alarmobjekte AO für die beiden Angriffserkennungssysteme S_A, S_B.

[00115] Zunächst wird für die erste Alarmobjektgruppe G_1, die das erste Alarmobjekt AO_1 des Alarmobjekttyps 1 von Angriffserkennungssystem S_A (Alarmobjekt-ID 1, Alarmobjekttyp Kreis) beinhaltet, ein erstes Alarmobjektmuster P_1 erstellt, da zu diesem Zeitpunkt noch kein Alarmobjektmuster vorhanden ist. Dies geschieht, indem die Alarmobjektgruppe, wie zuvor beschrieben, einer Datenbank D zugeordnet wird, durch die anschließend das Alarmobjektmuster P_1 erstellt wird.

[00116] Als nächstes wird die zweite Alarmobjektgruppe G_2, die das zweite Alarmobjekt AO_2 des Alarmobjekttyps 2 (Alarmobjekt-ID 2, Alarmobjekttyp Dreieck mit Spitze nach oben) beinhaltet,

betrachtet. Da es zu dem Zeitpunkt nur ein Alarmobjektmuster P_1 gibt, wird die Ähnlichkeit zwischen der zweiten Alarmobjektgruppe G_2 und dem ersten Alarmobjektmuster P_1 berechnet. Da keines der Attribute übereinstimmt, entspricht die Ähnlichkeit zwischen der zweiten Alarmobjektgruppe G_2 und dem ersten Alarmobjektmuster P_1 dem kleinstmöglichen Ähnlichkeitswert 0. Dieser Ähnlichkeitswert überschreitet nicht den vorgeschriebenen Alarmobjektgruppen-Ähnlichkeitsschwellenwert von t=0,5 und die Alarmobjektgruppe G_2 und das Alarmobjektmuster P_1 werden somit nicht als ähnlich betrachtet. Die zweite Alarmobjektgruppe G_2 wird deshalb der Wissensbasis D hinzugefügt, aus der ein zweites Alarmobjektmuster P_2, das zu diesem Zeitpunkt nur die zweite Alarmobjektgruppe G_2 umfasst, erstellt wird.

[00117] Das dritte Alarmobjekt AO_3 von Angriffserkennungssystem S_A ist wiederum vom Alarmobjekttyp 1 (Alarmobjekt-ID 3, Alarmobjekttyp Kreis) und in der dritten Alarmobjektgruppe G_3 gespeichert. Da es nun zwei Alarmobjektmuster P_1, P_2 gibt, wird die Ähnlichkeit zu beiden berechnet. Die Ähnlichkeit zwischen der dritten Alarmobjektgruppe G_3 und dem ersten Alarmobjektmuster P_1 ergibt den höchstmöglichen Ähnlichkeitswert von 1, da sowohl alle Attribute A, B, C in beiden vorhanden sind, als auch jeder Wert jedes Attributs (a, b, c) übereinstimmt. Die dritte Alarmobjektgruppe G_3 wird somit dem ersten Alarmobjektmuster P_1 zugeordnet. Dies geschieht, indem die Alarmobjektgruppe G_3 in der Datenbank D dem ersten Alarmobjektmuster P_1 zugeordnet wird, und dieses Alarmobjektmuster P_1 wird dann neu aus allen Alarmobjektgruppen G_1, G_3, die ihm in der Datenbank D zugeordnet sind, generiert. Da die beiden ihm zugehörigen Alarmobjektgruppen G_1, G_3 in der Datenbank D ident sind (beide Alarmobjektgruppen G_1, G_3 beinhalten jeweils einen Alarmobjekt AO_1, AO_3 des Alarmobjekttyps Kreis mit identen Attributen und Werten), bleibt das Alarmobjektmuster P_1 auch nach erneuter Generierung unverändert.

[00118] Die beiden folgenden Alarmobjektgruppen mit Alarmobjekt-ID 4 (Alarmobjekttyp Dreieck mit Spitze nach oben) und Alarmobjekt-ID 5 (Alarmobjekttyp Kreis) werden in gleicher Weise jeweils dem zweiten Alarmobjektmuster P_2 und dem ersten Alarmobjektmuster P_1 zugeordnet. Die sechste Alarmobjektgruppe G_6, die das Alarmobjekt mit Alarmobjekt-ID 6 (Alarmobjekttyp Dreieck mit Spitze nach unten) beinhaltet, weist einen anderen Wert bei Attribut Z auf, als alle bisherigen Alarmobjektgruppen.

[00119] Bei der Berechnung des Ähnlichkeitswertes zum ersten Alarmobjektmuster P_1 kommt es wie bei der zweiten Alarmobjektgruppe G_2 zu einem Ähnlichkeitswert von 0, da keines der Attribute übereinstimmt. Bei der Berechnung des Ähnlichkeitswertes zum zweiten Alarmobjektmuster P_2 jedoch stimmen zwar alle Attribute überein, nicht jedoch der Wert des Attributs Z, da im zweiten Alarmobjektmuster das Attribute den Wert z1 annimmt, in der Alarmobjektgruppe jedoch den Wert z3.

[00120] Für dieses Ausführungsbeispiel wird vereinfacht davon ausgegangen, dass sowohl eine Übereinstimmung der Attribute als auch eine Übereinstimmung der Werte gleichermaßen zum Ähnlichkeitswert beiträgt, so ergeben sich 5 von 6 möglichen Übereinstimmungen und somit ein Ähnlichkeitswert von 5/6 = 0,83. Da dieser Wert den vorgegebenen Alarmobjektgruppen-Ähnlichkeitsschwellenwert t=0,5 überschreitet und auch größer als der Ähnlichkeitswert zum ersten Alarmobjektmuster P_1 ist, wird die sechste Alarmobjektgruppe G6 dem zweiten Alarmobjektmuster P_2 zugeordnet. Dabei wird sie in der Datenbank D dem zweiten Alarmobjektmuster P_2 zugeordnet, das zu diesem Zeitpunkt die zweite und vierte Alarmobjektgruppe G_2, G_4 umfasst. Aus diesen drei Alarmobjektgruppen G_2, G_4, G_6 wird dann das Alarmobjektmuster P_2 neu generiert.

[00121] Dabei werden alle Attribute einzeln aggregiert. Da Attribute X und Y in allen Alarmobjektgruppen in den Werten übereinstimmen, werden diese unverändert in das Alarmobjektmuster P2 übernommen. Da das Attribut Z in den Alarmobjektgruppen G_2, G_4, G_6 zwei unterschiedliche Werte aufweist, nämlich z1 und z3, werden diese Werte als Liste im zweiten Alarmobjektmuster P_2 aufgenommen. Es ergibt sich somit zu diesem Zeitpunkt die in Fig. 9 schematisch dargestellte Struktur der Alarmobjektmuster P_1, P_2 (siehe Tabelle 3), wobei zu beachten ist, dass das repräsentative Alarmobjekt RA_2 des zweiten Alarmobjektmusters P_2 als Mischtyp dargestellt wird, der sowohl ein Dreieck mit der Spitze nach oben als auch ein Dreieck mit der Spitze nach unten enthält:

[00122] Tabelle 3: Alarmobjektmuster P_1, P_2:

Alarmobjektmuster-ID	Zeitschritt	Attribut 1	Attribut 2	Attribut 3
1	*	A=a	B=b	C=c
2	*	X=x	Y=y	Z=z1,z3

[00123] Visuelle Darstellung der des ersten (links) und zweiten (rechts) Alarmobjektmusters P_1, P_2 siehe Fig. 9.

[00124] Die siebente Alarmobjektgruppe G_7 beinhaltet wiederum ein Alarmobjekt AO_7 des Alarmobjekttyps Kreis und wird gleichermaßen wie die vorherigen Alarmobjektgruppen G_1, G_3, die zum ersten Alarmobjektmuster P_1 zugeordnet wurden, behandelt.

[00125] Die achte Alarmobjektgruppe G_8 besitzt wiederum ein Alarmobjekt AO_8 des Alarmobjekttyps Dreieck mit Spitze nach rechts, der einen neuen Wert für Attribut Z innehat. Wie vorhin ist die Ähnlichkeit zum ersten Alarmobjektmuster P1 gleich 0. Wäre der Wert für das Attribut Z entweder z1 oder z3, so würde die Ähnlichkeit zum zweiten Alarmobjektmuster P_2 gleich 1 betragen, da sowohl z1 als auch z3 in Alarmobjektmuster bei Attribut Z vorhanden sind, und somit beide Werte als Übereinstimmung akzeptiert werden würden. Da jedoch in der achten Alarmobjektgruppe G8 das Attribut Z den Wert z2 annimmt, beträgt die Ähnlichkeit wie vorhin 0,83. Somit wird auch diese Alarmobjektgruppe G_8 in der Datenbank D dem zweiten Alarmobjektmuster P_2 zugeordnet und das Alarmobjektmuster P_2 neu generiert. Die Attribute X und Y bleiben wie vorhin unverändert, nur bei Attribut Z sind nun drei verschiedene Werte vorhanden. Da die Maximalgröße der Liste an Werten, die einem Attribut eines repräsentativen Alarmobjekts RA zugeordnet werden können, mit 2 festgelegt wurde, wird der Wert des Attributs Z mit einem Platzhalter, symbolisiert durch einen Stern, ersetzt. Von nun an führt jeder Wert des Attributs Z zu einer Übereinstimmung.

[00126] Als nächstes wird die sechzehnte Alarmobjektgruppe G_{16}, die ein Alarmobjekt AO_{16} des Alarmobjekttyps Dreieck mit Spitze nach links beinhaltet und die in Alarmerkennungssystem S_B auftritt, betrachtet, die in Alarmerkennungssystem S_B auftritt. Die Ähnlichkeit zum ersten Alarmobjektmuster P_1 beträgt wie bei anderen Alarmobjektgruppen des Alarmobjekttyps 2 gleich 0.

[00127] Beim Vergleich mit dem zweiten Alarmobjektmuster P_2 fällt auf, dass wiederum ein neuer Wert für das Attribut Z, nämlich z4, auftritt. Da jedoch der zweite Alarmobjektmuster P_2 bereits für das Attribut Z über einen Platzhalter verfügt und somit der Wert z4 zu einer Übereinstimmung führt, sowie auch alle anderen Attribute und Werte übereinstimmen, ist die Ähnlichkeit zwischen der sechzehnten Alarmobjektgruppe G_{16} und dem zweiten Alarmobjektmuster P_2 gleich 1. Die Alarmobjektgruppe G_{16} wird demnach in der Datenbank D dem zweiten Alarmobjektmuster P_2 hinzugefügt. Bei der Neugenerierung des zweiten Alarmobjektmusters P_2 entsteht für das Attribut Z wiederum ein Platzhalter, da nun bereits vier verschiedene Werte in den in der Datenbank D gespeicherten zugehörigen Alarmobjektgruppen vorhanden sind.

[00128] Diese Prozedur wird für alle restlichen Alarmobjektgruppen G fortgesetzt, wobei sich die Alarmobjektmuster P_1, P_2 nicht weiter ändern. Aufgrund der hohen Ähnlichkeit von Alarmobjekten des Alarmobjekttyps 1, der hohen Ähnlichkeit von Alarmobjekten des Alarmobjekttyps 2, und der hohen Unähnlichkeit zwischen Alarmobjekten des Alarmobjekttyps 1 und Alarmobjekten des Alarmobjekttyps 2, existieren nach Bearbeitung aller restlichen Alarmobjekte zwei Alarmobjektmuster P_1, P_2, dabei steht jeweils ein Alarmobjektmuster für einen Alarmobjekttyp. Die Alarmobjektmuster P_1, P_2 sind wie in Tabelle 4 zusammengefasst:

[00129] Tabelle 4: Alarmobjektmuster P_1, P_2:

Alarmobjektmuster-ID	**Zeitschritt**	**Attribut 1**	**Attribut 2**	**Attribut 3**
1	*	A=a	B=b	C=c
2	*	X=x	Y=y	Z=*

[00130] Visuelle Darstellung der Alarmobjektmuster P_1, P_2 siehe Fig. 10.

[00131] In dieser, oben angeführten, detaillierten Beschreibung des zweiten Ausführungsbeispiels wurden unbeschränkt befüllbaren Listen verwendet.

[00132] Beispielhaft wird die Vorgehensweise nun auch für die beiden anderen zuvor erwähnten Strategien der Alarmobjektgruppenspeicherung erklärt. Bei der Strategie der linear befüllbaren Listen wird ein Fixwert für die maximale Alarmobjektgruppengröße vorgegeben. Ist dieser Fixwert größer als die maximal erreichte Alarmobjektgruppengröße, so gibt es keinen Unterschied zur Strategie der unbeschränkt befüllbaren Listen. Im vorher erklärten Anwendungsbeispiel entspricht das einem Fixwert von 12 oder mehr, da am Ende des Beispiels beide Alarmobjektmuster P_1, P_2 über Listen der Größe 12 in der Datenbank D verfügen.

[00133] Beispielhaft wird der Fixwert der Maximalgrößen der Listen mit 4 angenommen. Da der Alarmobjekttyp 1 wie im vorher erklärten zweiten Ausführungsbeispiel ersichtlich keinen Änderungen unterworfen ist, wird nur der Alarmobjekttyp 2 betrachtet. Zunächst wird die linear befüllbare Liste solange befüllt, bis der Maximalwert erreicht ist. Das ist der Fall, sobald die dem zweiten Alarmobjektmuster P_2 zugehörige Liste die Alarmobjektgruppen beinhaltet, die jeweils Alarmobjekte mit Alarmobjekt-ID 2, 4, 6, und 8 umfassen. Da die Vorgehensweise bis zu diesem Zeitpunkt gleich wie die Vorgehensweise mit unbeschränkt befüllbaren Listen ist, existiert zu diesem Zeitpunkt das zweite Alarmobjektmuster mit einem Platzhalter für Attribut Z.

[00134] Sobald das Alarmobjekt AO_{10} mit Alarmobjekt-ID 10 prozessiert wird, wird dieses, da es aufgrund des Platzhalters im zweiten Alarmobjektmuster P_2 eine perfekten Ähnlichkeitswert von 1 erreicht, zu der dem zweiten Alarmobjektmuster P_2 zugehörigen Liste an Alarmobjektgruppen hinzugefügt, die damit allerdings den Maximalwert der Listen überschreitet. Wie von der Strategie für linear befüllbare Listen vorgeschrieben, wird die älteste Alarmobjektgruppe, also die Alarmobjektgruppe die das Alarmobjekt mit Alarmobjekt- ID 2 umfasst, aus der Liste entfernt, sodass die resultierende Liste wieder eine Größe von 4 erreicht. Wird nun der zweite Alarmobjektmuster P_2 anhand dieser Alarmobjektgruppen aktualisiert, so besitzt der resultierende Alarmobjektmuster P_2 nach wie vor einen Platzhalter für Attribut Z, da für dieses Attribut drei verschiedene Werte vorkommen.

[00135] Dieses Vorgehen kann nun auch für alle restlichen Alarmobjekte AO durchgeführt werden. Die folgende Aufzählung (siehe Tabelle 5) zeigt dabei in jeder Zeile die in den Listen gespeicherten Alarmobjekte, wobei zur einfacheren Darstellung nur die Alarmobjekt-ID und die Richtung des Dreiecks von Alarmobjekttyp 2 genannt wird, und die damit einhergehende Veränderung des zweiten Alarmobjektmusters:

[00136] Tabelle 5: Attribute von Alarmobjektmuster P_2 und Listeneinträge

	Listeneinträge (nur Alarmobjekttyp 2)				Attribute von zweitem Alarmobjektmuster P_2		
Zeitschritt	1.	2.	3.	4.	X	Y	Z
3	2 (oben)	-	-	-	x	y	z1
9	2 (oben)	4 (oben)	-	-	x	y	z1
34	2 (oben)	4 (oben)	6 (unten)	-	x	y	z1, z3
40	2 (oben)	4 (oben)	6 (unten)	8 (rechts)	x	y	*
113	4 (oben)	6 (unten)	8 (rechts)	10 (oben)	x	y	*

119	6 (unten)	8 (rechts)	10 (oben)	12 (oben)	x	y	*
145	8 (rechts)	10 (oben)	12 (oben)	14 (unten)	x	y	*
151	10 (oben)	12 (oben)	14 (unten)	16 (links)	x	y	*
217	12 (oben)	14 (unten)	16 (links)	18 (oben)	x	y	*
223	14 (unten)	16 (links)	18 (oben)	20 (oben)	x	y	*
249	16 (links)	18 (oben)	20 (oben)	22 (unten)	x	y	*
255	18 (oben)	20 (oben)	22 (unten)	24 (unten)	x	y	z1, z3

[00137] Obenstehende Aufzählung zeigt, dass sich über lange Zeit (Zeitschritte 40-249) das zweite Alarmobjektmuster P_2 mit einem Platzhalter für Attribut Z ergibt. Jedoch wird in Zeitschritt 255 dieser Platzhalter wieder durch eine Liste ersetzt, da die vier, in der dem Alarmobjektmuster P_2 zugehörigen Liste gespeicherten, Alarmobjektgruppen nur Alarmobjekte beinhalten, die bei Attribut zwei verschiedene Werte, z1 und z3, annehmen, und somit nicht die notwendige Diversität erreichen, um durch einen Platzhalter ersetzt zu werden.

[00138] In manchen Fällen ist dieser Effekt vorteilhaft, da dadurch erreicht wird, dass möglicherweise inkorrekt hinzugefügte Alarmobjektgruppen aus dem Alarmobjektmuster P_2 herausaltern. In diesem Fall jedoch hat sich der Platzhalter über lange Zeit und mehrere Hinzufügeoperationen von Alarmobjektgruppen als korrekt erwiesen und sollte somit beibehalten werden. Dies kann erreicht werden, indem die maximale Größe der Listen erhöht wird, zum Beispiel von 4 auf 5, wodurch ausreichend große Diversität von Attributen erreicht wird.

[00139] Als nächstes wird die Strategie der logarithmisch befüllbaren Listen diskutiert. Wie bei der Strategie der linear befüllbaren Listen, wird die maximale Größe der Listen mit 4 festgelegt. Da es sich um eine auf dem Zufall basierende Auswahl von Alarmobjektgruppen handelt, kann nur ein beispielhafter Prozessablauf gezeigt werden. Das Hinzufügen der Alarmobjektgruppen und beinhalteten Alarmobjekte mit Alarmobjekt-ID 2, 4, 6, und 8 zu der dem zweiten Alarmobjektmuster zugehörigen Liste ist ident zu den anderen Strategien. Das Hinzufügen der Alarmobjektgruppe, die Alarmobjekt mit Alarmobjekt-ID 10 beinhaltet, könnte die zuletzt hinzugefügte Alarmobjektgruppe ersetzen, da dies in 50% aller Fälle geschieht.

[00140] In dem Fall verändert sich Attribut Z im Alarmobjektmuster zu einer Liste die z1 und z3 beinhaltet, da der Wert z2 überschrieben wurde. Die Alarmobjektgruppe, die Alarmobjekt mit Alarmobjekt-ID 12 beinhaltet, könnte die letzten beiden Alarmobjektgruppen in Richtung der ersten Position verschieben und an der letzten Position eingefügt werden, da dies in 12,5% aller Fälle geschieht. Die Alarmobjektgruppe, die das Alarmobjekt mit Alarmobjekt-ID 13 beinhaltet, könnte die letzte Alarmobjektgruppe in Richtung der ersten Position verschieben und an der letzten Position eingefügt werden, da dies in 25% aller Fälle geschieht. Die folgende Tabelle 6 stellt diese und darauffolgende Operationen dar:

[00141] Tabelle 6: Attribute von Alarmobjektmuster P_2 und Listeneinträge

	Listeneinträge (nur Alarmobjekttyp 2)				Attribute von zweitem Alarmobjektmuster P_2		
Zeitschritt	1.	2.	3.	4.	X	Y	Z
3	2 (oben)	-	-	-	x	y	z1
9	2 (oben)	4 (oben)	-	-	x	y	z1
34	2 (oben)	4 (oben)	6 (unten)	-	x	y	z1, z3
40	2 (oben)	4 (oben)	6 (unten)	8 (rechts)	x	y	*
113	2 (oben)	4 (oben)	6 (unten)	10 (oben)	x	y	z1, z3
119	2 (oben)	6 (unten)	10 (oben)	12 (oben)	x	y	z1, z3
145	2 (oben)	6 (unten)	10 (oben)	14 (unten)	x	y	z1, z3
151	2 (oben)	6 (unten)	10 (oben)	16 (links)	x	y	*

217	6 (unten)	10 (oben)	16 (links)	18 (oben)	x	y	*
223	6 (unten)	10 (oben)	16 (links)	20 (oben)	x	y	*
249	6 (unten)	16 (links)	20 (oben)	22 (unten)	x	y	*
255	6 (unten)	16 (links)	20 (oben)	24 (unten)	x	y	*

[00142] Wie in der Auflistung zu sehen ist, besteht die Liste der dem zweiten Alarmobjektmuster zugeordneten Alarmobjektgruppen aus verschiedenen Alarmobjektgruppen, die über einen langen Zeitraum aufgetreten sind. Insbesondere befinden sich eine Alarmobjektgruppe von System A und drei Alarmobjektgruppen von System B in dieser Wissensbasis. Somit stellt diese Liste eine Stichprobe dar, die repräsentativer für systemübergreifende Alarmobjektgruppen ist, als eine linear befüllbare Liste, und hat den Vorteil einer geringeren Rechenlaufzeit sowie geringeren benötigten Speicherbedarf als eine unbeschränkte Liste. Da es sich um eine statistische Befüllung der Liste handelt, ist jedoch nicht garantiert, dass die resultierenden Alarmobjektmustere in jeder Ausführung ident sind.

[00143] Aus Gründen der Einfachheit wird im Folgenden ausschließlich die Strategie der unbeschränkten Listen erklärt. Die anderen Strategien können analog zum vorher erklärten Beispiel angewandt werden. Als nächstes wird die Zeitspanne 10 Sekunden betrachtet, die in Abb. Fig. 5 dem kleinen zeitlichen Abstandsschwellenwert δ_{small} entspricht. Für diese Zeitspanne werden die zuvor gefundenen Alarmobjektmuster nicht berücksichtigt.

[00144] Alarmobjekte, die sich in einem Abstand von weniger als 10 Sekunden zu einem anderen Alarmobjekt oder einer Alarmobjektgruppe befinden, werden in einer oder dieser Alarmobjektgruppe zusammengefasst. Es entstehen somit zwei Alarmobjektgruppen G_1, G_2 in Angriffserkennungssystem S_A und vier Alarmobjektgruppen G_3, ..., G_6 in Angriffserkennungssystem S_B, die jeweils vier Alarmobjekte AO umfassen. Die Alarmobjektgruppen G_1, ..., G_6 sind in Fig. 11 abgebildet.

[00145] Am Beginn des Ablaufs eines erfindungsgemäßen Verfahrens sind wiederum keine Alarmobjektmuster P vorhanden. Die erste Alarmobjektgruppe G_1, die Alarmobjekte AO_1, ..., AO_4 mit Alarmobjekt-ID 1 bis 4 umfassen, wird deshalb in eine neue Datenbank D eingefügt (Schritt (1) in Fig. 5), und ein neues Alarmobjektmuster P_1 wird aus dieser Alarmobjektgruppe G_1 generiert (Schritt (2) in Fig. 5).

[00146] Die zweite Alarmobjektgruppe G_2 umfasst Alarmobjekte AO_5, ..., AO_8 mit Alarmobjekt-ID 5 bis 8 und wird mit dem Alarmobjektmuster P_1 verglichen (Schritt (3) in Fig. 5). Da die Alarmobjektgruppe G_2 und das Alarmobjektmuster P_1 jeweils mehrere Alarmobjekte AO_5, ..., AO_8 bzw. repräsentative Alarmobjekte RA_1, ..., RA_4 aufweisen, wird zunächst eine Zuordnung zwischen den Alarmobjekten AO_5, ..., AO_8 und repräsentativen Alarmobjekten RA_1, ..., RA_4 gesucht, die auf der Ähnlichkeit der Alarmobjekte basiert.

[00147] Unter der Annahme, dass das erste Alarmobjekt AO_5 der zweiten Alarmobjektgruppe G_2 mit dem ersten repräsentativen Alarmobjekt RA_1 des Alarmobjektmusters P_1 verglichen wird, das zweite Alarmobjekt AO6 der zweiten Alarmobjektgruppe G_2 mit dem zweiten repräsentativen Alarmobjekt RA_2 des Alarmobjektmusters P_1, usw., dann ergibt sich für die Paarung des ersten Alarmobjekts AO_5 der zweiten Alarmobjektgruppe G_2 mit dem ersten repräsentativen Alarmobjekt RA_1 des Alarmobjektmusters P_1 eine Ähnlichkeit von 1, da alle Attribute und Werte übereinstimmen. Für die Paarung des zweiten Alarmobjekts AO_6 der zweiten Alarmobjektgruppe G_2 mit dem zweiten repräsentativen Alarmobjekt RA_2 des Alarmobjektmusters P_1 eine Ähnlichkeit von 0,83, da sich die Werte des Attributs Z unterscheiden, für die Paarung des dritten Alarmobjekts AO_7 der zweiten Alarmobjektgruppe G_2 mit dem dritten repräsentativen Alarmobjekt RA_3 des Alarmobjektmusters P_1 eine Ähnlichkeit von 1, da alle Attribute und Werte übereinstimmen, und für die Paarung des vierten Alarmobjekts AO_8 der zweiten Alarmobjektgruppe G_2 mit dem vierten repräsentativen Alarmobjekt RA_4 des Alarmobjektmusters P_1 eine Ähnlichkeit von 0,83, da sich die Werte des Attributs Z unterscheiden.

[00148] Vorteilhafterweise würden an dieser Stelle alle Paarungen, deren Ähnlichkeit einen vorgegebenen Alarmobjekt-Ähnlichkeitsschwellenwert unterschreiten, ignoriert werden, um falsche Zuordnungen und in weiterer Folge inkorrekte Alarmobjektaggregationen, die im Zuge des Zusammenfassens bzw. Aggregierens von Alarmobjektgruppen durchgeführt werden und zu übergeneralisierten Alarmobjekten führen, zu vermeiden.

[00149] Die Ähnlichkeit der zweiten Alarmobjektgruppe G_2 zum Alarmobjektmuster P_1 wird beispielsweise als Durchschnitt der Ähnlichkeiten der Paarungen berechnet, also (1+0,83+1+0,83)/4 = 0,92. Da diese Ähnlichkeit den Schwellenwert von 0,5 übersteigt, wird die zweite Alarmobjektgruppe G_2 in der Datenbank D dem Alarmobjektmuster P_1 zugeordnet (Schritt (4) in Fig. 5) und das Alarmobjektmuster P_1 wird neu generiert (Schritt (5) in Fig. 5, wobei zu diesem Zeitpunkt nur die erste und zweite Alarmobjektgruppe G_1, G_2 in der Datenbank D vorhanden sind). Dabei wird beim zweiten repräsentativen Alarmobjekt RA_2 des Alarmobjektmusters P_1 für das Attribut Z eine Liste erzeugt, nämlich Z=z1,z3, da die zweiten Alarmobjekte der ersten und zweiten Alarmobjektgruppe G_1, G_2 jeweils die Werte z1 und z3 in Attribut Z annehmen und sich somit unterscheiden, sowie beim vierten repräsentative Alarmobjekt RA_4 des Alarmobjektmusters P_1 für das Attribut Z eine Liste erzeugt, nämlich Z=z1,z2, da die vierten Alarmobjekte der ersten und zweiten Alarmobjektgruppe G_1, G_2 jeweils die Werte z1 und z2 in Attribut Z annehmen und sich somit unterscheiden.

[00150] Es wird gleichermaßen für alle Alarmobjektgruppen G_3, ..., G_6 des Alarmerkennungssystems SB fortgefahren (wiederholtes Ausführen der Schritte (3)-(5) in Fig. 5, wobei jeweils die zu dem Zeitpunkt prozessierte Alarmobjektgruppe G_3, ..., G_6 verglichen und der Datenbank D hinzugefügt wird). Es zeigt sich, dass die Ähnlichkeiten aller Alarmobjektgruppen G_3, ..., G_6 zum Alarmobjektmuster P_1 den Alarmobjektgruppen-Ähnlichkeitsschwellenwert überschreiten, und somit alle Alarmobjektgruppen G_3, ..., G_6 in der Datenbank D des Alarmobjektmusters P_1 zugeordnet werden.

[00151] Auffallend ist, dass alle weiteren Alarmobjektgruppen G_3, ..., G_6 des Alarmerkennungssystems S_B für das zweite Alarmobjekt einen der Werte z1 und z3 im Attribut Z annehmen. Somit wird die Maximalgröße der Liste der aggregierten Alarmobjektgruppen des Alarmobjektmusters P_1 nicht überschritten. Anders ist es bei dem vierten Alarmobjekt in allen Alarmobjektgruppen G_3, ..., G_6 wo alle Werte z1, z2, z3, und z4 im Attribut Z angenommen werden. Dementsprechend wird dieser Wert wieder mit einem Platzhalter ersetzt. Es ergibt sich also nur ein Alarmobjektmuster P_1 (siehe Fig. 12), das wie in Tabelle 7 zusammengefasst lautet.

[00152] Tabelle 7: Alarmobjektmuster P1:

Alarmobjektmuster-ID	**Zeitschritt**	**Attribut 1**	**Attribut 2**	**Attribut 3**
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=z1,z3
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=*

[00153] Visuelle Darstellung des Alarmobjektmusters siehe Fig. 12 (entspricht dem Alarmobjektmuster des kleinen zeitlichen Abstandsschwellenwert δ_{small} in Abb. Fig. 5).

[00154] Abschließend werden die Alarmobjektgruppen für die Zeitspanne 50 Sekunden betrachtet. Dies entspricht dem großen zeitlichen Abstandsschwellenwert δ_{large} in Fig. 5. In Angriffserkennungssystem S_A ergibt sich nur eine einzige Alarmobjektgruppe G_1, in Angriffserkennungssystem S_B ergeben sich zwei Alarmobjektgruppen G_2, G_3. Die Alarmobjektgruppen G_1, ..., G_3 sind in Fig. 13 dargestellt.

[00155] Zuerst wird die erste und einzige Alarmobjektgruppe G_1 von Angriffserkennungssystem S_A der Datenbank D hinzugefügt und anhand der Alarmobjektgruppe G_1 ein neues Alarmobjektmuster P_1 generiert, da es wie vorhin zu diesem Zeitpunkt noch kein Alarmobjektmuster gibt.

[00156] Danach wird für die erste Alarmobjektgruppe G_2 von Angriffserkennungssystem S_B die Ähnlichkeit zum Alarmobjektmuster P_1 berechnet. Es ist in Fig. 13 ersichtlich, dass die ersten sieben Alarmobjekte AO_9, ..., AO_{15} der zweiten Alarmobjektgruppe G_2 und die ersten sieben Alarmobjekte AO_1, ..., AO_7 des Alarmobjektmusters P_1, das zu diesem Zeitpunkt der ersten und einzigen Alarmobjektgruppe G_1 von Angriffserkennungssystem S_A entspricht, einander entsprechen und somit jeweils in bestmöglichen Ähnlichkeiten, d.h., jeweils einer Ähnlichkeit von 1, zwischen diesen Alarmobjekten resultieren.

[00157] Das achte repräsentative Alarmobjekt RA_8 des Alarmobjektmusters P_1, das dem achten Alarmobjekt AO_8 der Alarmobjektgruppe G_1 entspricht, ist vom Alarmobjekttyp Dreieck mit der Spitze nach rechts, während das achte Alarmobjekt AO_{16} der ersten Alarmobjektgruppe G_2 von Angriffserkennungssystem S_B vom Typ Dreieck mit Spitze nach links ist. Wie vorhin wird die Ähnlichkeit dieser Alarmobjekte AO_8, AO_{16} mit 0,83 beziffert.

[00158] Der Durchschnitt über alle Alarmobjekte AO_1, ..., AO_8; AO_9, ..., AO_{16} und somit die Ähnlichkeit der Alarmobjektgruppen G_1, G_2 beläuft sich auf (1+1+1+1+1+1+1+0,83)/8 = 0,98. Da diese Ähnlichkeit den Schwellenwert von 0,5 überschreitet, wird die erste Alarmobjektgruppe G_2 von Angriffserkennungssystem S_B in der Datenbank D dem Alarmobjektmuster P_1 zugeordnet. Wie vorhin wird das Alarmobjektmuster P_1 neu generiert, wobei der achte repräsentative Alarmobjekt RA_8 als Mischtyp des Dreiecks mit der Spitze nach rechts und des Dreiecks mit der Spitze nach links erzeugt wird.

[00159] Die zweite Alarmobjektgruppe G_3 von Angriffserkennungssystem S_B wird analog behandelt. Da sich wiederum diese Alarmobjektgruppe G_3 mit dem Alarmobjektmuster P_1 nur an der achten Position der Alarmobjektsequenz unterscheidet, wird erneut eine Ähnlichkeit von 0,98 erreicht. Die Alarmobjektgruppe G_3 wird also in der Datenbank D dem Alarmobjektmuster P1 zugeordnet und das Alarmobjektmuster P_1 besitzt nach Neugenerierung an der achten Position der Alarmobjektsequenz ein repräsentatives Alarmobjekt RA_8 vom Alarmobjekttyp Dreieck (siehe Fig. 14), wobei das Attribut Z als Platzhalter vorhanden ist, da sich bereits drei verschiedene Werte in den achten Positionen der Alarmobjektsequenzen der drei Alarmobjektgruppen G_1, ..., G_3 in der Datenbank D befinden.

[00160] Wie vorhin bildet sich nach Prozessierung aller Alarmobjektgruppen G_1, ..., G_3 also nur ein einziges Alarmobjektmuster P_1, da alle Alarmobjektgruppen die notwendige Ähnlichkeit zu dem schrittweise generierten Alarmobjektmuster P_1 erreichen. Das Alarmobjektmuster P_1 ist in Fig. 14 und Tabelle 8 dargestellt.

[00161] Tabelle 8: Schrittweise Erstellung des Alarmobjektmusters P1:

Meta-ID	**Zeitschritt**	**Attribut 1**	**Attribut 2**	**Attribut 3**
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=z1
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=z1
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=z3
1	*	A=a	B=b	C=c
1	*	X=x	Y=y	Z=*

[00162] Visuelle Darstellung des Alarmobjektmusters siehe Fig. 14 (entspricht dem Alarmobjektmuster des großen zeitlichen Abstandsschwellenwert δ_{large} in Abb. Fig. 5).

[00163] Es ist anzumerken, dass sich die erstellten Alarmobjektmuster P stark unterscheiden können, je nachdem, welcher zeitliche Abstandsschwellenwert δ gewählt wird. Das betrifft sowohl die Anzahl der Alarmobjekte AO im Alarmobjektmuster P, als auch deren Attribute nach der Aggregation. Es ist daher vorteilhaft, mehrere zeitliche Abstandsschwellenwert δ parallel anzuwenden, um von verschiedenen Angriffstypen unterschiedliche Arten von Alarmobjektmustern P ab-

zuleiten, um somit die Wahrscheinlichkeit zu erhöhen, dass zumindest eines dieser Alarmobjektmuster P ermöglicht, ein konkretes Vorkommen eines ähnlichen oder variierten Angriffs wiederzuerkennen.

[00164] Dies beendet das zweite Ausführungsbeispiel eines beispielhaften Prozessablaufs eines erfindungsgemäßen Verfahrens. Um das Ausführungsbeispiel simpel zu halten, wurden Alarmobjekte AO mit einem einfachen Aufbau verwendet, insbesondere mit jeweils drei Attributen, wobei zwei Attribute bei jedem Alarmobjekttyp konstant sind. Weiters treten alle Alarmobjekte AO in der korrekten Reihenfolge auf, um die Zuordnungen zu vereinfachen. Um zusätzlich die Berechnung der Ähnlichkeit zwischen Alarmobjekten AO und Alarmobjektgruppen G sowie die Aggregation von Alarmobjekten AO und Alarmobjektgruppen G im Detail zu erklären, werden im Folgenden beispielhaft die Ähnlichkeitsmetriken und Zusammenfassungs- bzw. Aggregationsmethoden erklärt. Dabei sind die genannten Ausführungsbeispiele unabhängig von den zuvor erklärten Ausführungsbeispielen.

AUSFÜHRUNGSBEISPIEL - ÄHNLICHKEITSMETRIK FÜR ALARMOBJEKTE

[00165] Im Folgenden wird eine beispielhafte Ähnlichkeitsmetrik für Alarmobjekte AO erklärt. Alarmobjekte AO werden als semi-strukturierte Objekte angesehen. Eine semi-strukturierte Darstellung von Alarmobjekten AO ist auch in der Praxis üblich (siehe z.B. OSSEC Alarme im JSON Format (https://ossec-docs.readthedocs.io/en/latest/docs/formats/alerts.html#sample-alerts-json-messages, zuletzt aufgerufen am 17.11.2020).

[00166] Sollten Alarmobjekte AO in strukturierter Form vorliegen, lässt sich die Metrik ebenfalls anwenden, da jedes strukturierte Alarmobjekt AO auch als semi-strukturiertes Alarmobjekt AO darstellbar ist.

[00167] Entsprechend der semi-strukturierten Eigenschaften werden im Folgenden Alarmobjekte AO als Objekte dargestellt, die über eine bestimmte Anzahl an Attributen verfügen, wobei zu jedem Attribut ein bestimmter Wert gespeichert wird. Werte können dabei entweder simple Werte wie Zahlen oder Zeichenketten darstellen, oder komplexe Strukturen annehmen, wie Listen von Zahlen oder Zeichenketten, die mit eckigen Klammern gekennzeichnet sind, oder auch verschachtelte Objekte, die mit geschwungenen Klammer gekennzeichnet sind.

[00168] Weiters ist es möglich, dass Attribute die vorher erwähnten Strukturen von aggregierten Listen, die mit spitzen Klammern gekennzeichnet sind, und Platzhalter, die mit einem Stern gekennzeichnet sind, speichern. Im Folgenden werden zwei Beispiel Alarmobjekte Alarmobjekt1 (AO_1) und Alarmobjekt2 (AO_2) betrachtet, die verschiedene dieser Attribute beinhalten.

AO_1 = {

```
  "A": "a",
  "B": "b1",
  "C": ["c1", "c2"],
  "D": {
    "D1": "d1",
    "D2": "d2"
  },
  "E": "e2",
  "F": "f4",
  "G": "g8"
}
```

AO_2 = {

```
  "A": "a",
```

```
  "B": "b2",
  "C": ["c1"],
  "D": {
    "D1": "d1"
  },
  "E": <"e1","e2","e3">,
  "F": <"f1","f2","f3">,
  "G": *
}
```

[00169] Die Ähnlichkeit zwischen AO_1 und AO_2 soll bestimmt werden. Die Ähnlichkeitsmetrik vergleicht dazu alle Attribute der beiden Alarmobjekte AO_1 und AO_2 und zählt dazu die Anzahl der Übereinstimmungen sowie die Anzahl der Unterschiede.

[00170] Das Attribut A ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden und besitzt den gleichen Wert a, die Anzahl der Übereinstimmungen erhöht sich um 1 auf 1. Das Attribut B ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden, nimmt allerdings den Wert b1 in Alarmobjekt1 und b2 in Alarmobjekt AO_2 an. Deshalb erhöht sich die Anzahl der Unterschiede um 1 auf 1.

[00171] Das Attribut C ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden, ist jedoch eine Liste mit zwei Elementen in Alarmobjekt AO_1 und eine Liste mit nur einem Element in Alarmobjekt AO_2. Da ein Element der Liste, c1, in beiden Alarmobjekten AO_1 und AO_2 übereinstimmt, und somit die Hälfte der Liste übereinstimmt, werden die Übereinstimmungen um 0,5 auf 1,5 erhöht. Da ein Element der Liste in Alarmobjekt AO_1 nicht in der Liste von Alarmobjekt AO_2 vorhanden ist, und somit die Hälfte der Liste nicht übereinstimmt, wird die Anzahl der Unterschiede um 0,5 auf 1,5 erhöht.

[00172] Das Attribut D ist in beiden Alarmobjekten AO_1 und AO_2 ein verschachteltes Objekt. Jedes Attribut im verschachtelten Objekt wird als normales Attribut gehandhabt. Das Attribut D1 ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden und besitzt den gleichen Wert d1, die Anzahl der Übereinstimmungen erhöht sich um 1 auf 2,5. Das Attribut D2 ist nur in Alarmobjekt AO_1 vorhanden, nicht aber in Alarmobjekt AO_2. Um fehlende Attribute höher zu gewichten als unterschiedliche Werte bei gleichen Attributen, wird die Anzahl der Unterschiede um 1,5 auf 3 erhöht.

[00173] Das Attribut E ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden, und ist in Alarmobjekt AO_2 eine aggregierte Liste. Das bedeutet, dass auch eine Teilmenge der Liste als Wert ausreicht, um als Übereinstimmung zu gelten. Da der Wert von Alarmobjekt AO_1 in Attribut E gleich e2 ist, und e2 ein Teil der Liste von Attribut E in Alarmobjekt AO_2 ist, wird die Anzahl der Übereinstimmungen um 1 auf 3,5 erhöht.

[00174] Auch das Attribut F ist in beiden Alarmobjekten AO_1 und AO_2 vorhanden und in Alarmobjekt AO_2 eine aggregierte Liste, jedoch ist der Wert f4 von Alarmobjekt AO_1 nicht in der Liste enthalten. Deshalb wird die Anzahl der Unterschiede um 1 auf 4 erhöht. Das Attribut G ist ebenfalls in beiden Alarmobjekten vorhanden und weist einen Platzhalter in Alarmobjekt AO_2 auf. Daher ist egal, welchen Wert das Attribut G in Alarmobjekt1 einnimmt, die Anzahl der Übereinstimmungen wird auf jeden Fall um 1 auf 4,5 erhöht.

[00175] Somit ist die finale Anzahl der Übereinstimmungen 4,5 und die finale Anzahl der Unterschiede 4. Die Ähnlichkeit wird durch das Verhältnis der Übereinstimmungen und der Summe der Übereinstimmungen und Unterschiede ermittelt, also 4,5/(4,5+4) = 0,53.

AUSFÜHRUNGSBEISPIEL - AGGREGATIONSMETRIK FÜR ALARMOBJEKTE AO

[00176] Im Folgenden wird eine beispielhafte Aggregationsmetrik für Alarmobjekte AO erklärt. Wie vorhin sind Alarmobjekte AO semi-strukturierte Objekte. Es werden folgende Alarmobjekte betrachtet:

AO_3 = {
"A": "a1",
"B": "b1",
"C": "c1",
"D": "d1"
}

AO_4 = {
"A": "a1",
"B": "b2",
"C": "c2"
}

AO_5 = {
"A": "a1",
"B": "b1",
"C": "c3"
}

[00177] Die drei Alarmobjekte AO_3, AO_4, AO_5 sollen aggregiert werden. Dazu werden folgende Parameter verwendet. Die Maximalgröße der aggregierten Listen beträgt 2 und das minimale relative Auftreten eines Attributes beträgt 0,4.

[00178] Es werden alle Attribute getrennt betrachtet. Das Attribut A ist in allen Alarmobjekten AO_3, AO_4, AO_5 vorhanden und hat in allen Alarmobjekten AO_3, AO_4, AO_5 den gleichen Wert a1. In einem aggregierten Alarmobjekt bzw. repräsentativen Alarmobjekt RA eines Alarmobjektmusters P wird das Attribut A deshalb als aggregierte Liste mit nur einem Element a1 erzeugt.

[00179] Das Attribut B ist in allen Alarmobjekten AO_3, AO_4, AO_5 vorhanden und nimmt dabei zweimal die Werte b1 und einmal den Wert b2 an. Da somit zwei verschiedene Werte vorliegen, wird im aggregierten Alarmobjekt das Attribut B als aggregierte Liste mit den zwei Werten b1 und b2 gespeichert.

[00180] Das Attribut C ist in allen Alarmobjekten AO_3, AO_4, AO_5 vorhanden und nimmt dabei die Werte c1, c2, und c3 an. Da somit drei verschiedene Werte vorliegen, und diese Anzahl die Maximalgröße der aggregierten Listen überschreitet, wird das Attribut C mit einem Platzhalter im aggregierten Alarmobjekt hinzugefügt.

[00181] Das Attribut D kommt nur in Alarmobjekt AO_3 vor. Somit ist es nur in einem von 3 Alarmobjekten vorhanden, das heißt, die relative Häufigkeit 0,33 ist kleiner als das minimale relative Auftreten 0,4 und das Attribut wird somit nicht in das aggregierte Alarmobjekt übernommen. Das aggregierte Alarmobjekt sieht somit folgendermaßen aus:

AO_6 = {
"A": <"a1”>,
"B": <”b1”,"b2">,
"C": *
}

AUSFÜHRUNGSBEISPIEL - ÄHNLICHKEITSMETRIK FÜR KLEINE ALARMOBJEKTGRUPPEN G

[00182] Im Folgenden wird eine Ähnlichkeitsmetrik für Alarmobjektgruppen G beispielhaft erklärt. Dafür werden die folgenden zwei Alarmobjektgruppen G_1, G_2 definiert.

G_1 = { AO_1, AO_3, AO_5}

G_2 = {AO_5, AO_2, AO_4, AO_4}

[00183] Die erste Alarmobjektgruppe G1 besteht somit aus drei Alarmobjekten AO_1, AO_3, AO_5, die zweite Alarmobjektgruppe G_2 besteht aus vier Alarmobjekten AO_5, AO_2, AO_4, AO_4. Dabei ist Alarmobjekt AO_5 in beiden Alarmobjektgruppen G_1, G_2 vorhanden, Alarmobjekt AO_4 ist doppelt in der zweiten Alarmobjektgruppe G_2 vorhanden.

[00184] Es wird wieder die zuvor beschriebene Ähnlichkeitsmetrik verwendet, die alle Alarmobjekte AO miteinander vergleicht. Im Folgenden wird die Ähnlichkeit jeder Kombination aus Alarmobjekten AO aus den beiden Alarmobjektgruppen G_1, G_2 genannt, wobei die Ähnlichkeit zwischen AO_1 und AO_2 wie im Ausführungsbeispiel Ähnlichkeitsmetrik für Alarmobjekte durchgeführt wird, alle anderen Ähnlichkeiten analog berechnet werden, und idente Paarungen nicht doppelt genannt werden.

Ähnlichkeit von AO_1 und AO_5: 0,1
Ähnlichkeit von AO_1 und AO_2: 0,53
Ähnlichkeit von AO_1 und AO_4: 0,1
Ähnlichkeit von AO_3 und AO_5: 0,44
Ähnlichkeit von AO_3 und AO_2: 0,12
Ähnlichkeit von AO_3 und AO_4: 0,22
Ähnlichkeit von AO_5 und AO_5: 1,0
Ähnlichkeit von AO_5 und AO_2: 0,0
Ähnlichkeit von AO_5 und AO_4: 0,33

[00185] Es werden nun die besten Übereinstimmungen, d.h., die Paarungen, die die höchste Ähnlichkeit erzielen, zwischen allen Alarmobjekten AO gesucht, wobei jedes Alarmobjekt AO nur in einer Paarung auftreten darf. Dazu werden zuerst die Paarungen absteigend nach Ähnlichkeit sortiert.

Ähnlichkeit von AO_5 und AO_5: 1,0
Ähnlichkeit von AO_1 und AO_2: 0,53
Ähnlichkeit von AO_3 und AO_5: 0,44
Ähnlichkeit von AO_5 und AO_4: 0,33
Ähnlichkeit von AO_3 und AO_4: 0,22
Ähnlichkeit von AO_3 und AO_2: 0,12
Ähnlichkeit von AO_1 und AO_5: 0,1
Ähnlichkeit von AO_1 und AO_4: 0,1
Ähnlichkeit von AO_5 und AO_2: 0,0

[00186] Als nächstes wird von oben nach unten die Liste durchgegangen, und alle Paarungen entfernt, die Alarmobjekte AO beinhalten, die bereits in einer anderen Paarung vorhanden sind, wobei mehrfach auftretende Alarmobjekte AO entsprechend oft in den Paarungen vorkommen dürfen.

[00187] In diesem Fall wird die erste Paarung akzeptiert, da sie nur Alarmobjekt AO_5 umfasst, der in beiden Alarmobjektgruppen G_1, G_2 vorhanden ist. Die zweite Paarung wird ebenfalls akzeptiert, da Alarmobjekt AO_1 in Alarmobjektgruppe G_1 und Alarmobjekt AO_2 in Alarmobjektgruppe G_2 vorhanden sind.

[00188] Die dritte Paarung jedoch betrifft Alarmobjekt AO_5 in der zweiten Alarmobjektgruppe G_2, wobei dieses Alarmobjekt AO_5 schon in der ersten Paarung verwendet wurde. Deshalb wird die dritte Paarung entfernt. Selbiges gilt für die vierte Paarung. Erst die fünfte Paarung, die Alarmobjekt AO_3 in Alarmobjektgruppe G_1 und Alarmobjekt AO_4 in Alarmobjektgruppe G_2 betrifft, wird wieder akzeptiert. Da es keine weiteren noch nicht in Paarungen verwendeten Alarmobjekte in Alarmobjektgruppe G_1 gibt, kann an dieser Stelle abgebrochen werden. Die resultierenden Paarungen sind also wie folgt.

Ähnlichkeit von AO_5 und AO_5: 1,0

Ähnlichkeit von AO_1 und AO_2: 0,53
Ähnlichkeit von AO_3 und AO_4: 0,22

[00189] Weiters existiert ein zusätzlicher Alarmobjekt AO_4 in Alarmobjektgruppe G_2, der als nicht erfolgreiche Paarung mit der Ähnlichkeit 0 gilt. Die Ähnlichkeit der Alarmobjektgruppen G_1, G_2 ergibt sich aus dem Durchschnitt aller Paarungen, also (1,0+0,53+0,22+0)/4 = 0,44. Dieser Werte könnte noch modifiziert werden, indem die Reihenfolge der Paarungen berücksichtigt wird.

[00190] Da beispielsweise Alarmobjekt AO_5 in der ersten Alarmobjektgruppe G_1 an Position 3 steht, aber an Position 1 in der zweiten Alarmobjektgruppe G_2, sind zwei Verschiebungsoperationen notwendig, um die Alarmobjekte an die gleiche Position zu befördern. Da somit zwei der vier Positionen in Alarmobjektgruppe G_2 verändert werden müssen, beträgt die Ähnlichkeit der Reihenfolge nur (1-2/4)=0,5. Dieser Wert könnte gewichtet in den Alarmobjektgruppenähnlichkeitswert miteinfließen, bei einer gleich hohen Gewichtung wäre der resultierende Wert beispielsweise 0,44*0,5=0,22.

AUSFÜHRUNGSBEISPIEL - ÄHNLICHKEITSMETRIK FÜR GROßE ALARMOBJEKTGRUPPEN G

[00191] Da die Anzahl der Paarungen quadratisch mit den Alarmobjektgruppengrößen anwächst, ist die zuvor erklärte Ähnlichkeitsmetrik nur für kleine Alarmobjektgruppen G durchführbar. Wir erklären nun eine Ähnlichkeitsmetrik für große Alarmobjektgruppen G anhand der folgenden Alarmobjektgruppen G_3 (Alarmobjektgruppe3), G_4 (Alarmobjektgruppe4), wobei die Zahlen angeben, wie oft der jeweilige Alarmobjekt AO in der Alarmobjektgruppe G_3, G_4 vorkommt, und Paare von Zahlen angeben, in welchem Bereich die Anzahl der vorkommenden Alarmobjekte AO des jeweiligen Typs vorkommen kann, d.h., im folgenden Beispiel kommt Alarmobjekt AO_1 in Alarmobjektgruppe G_3 genau 1000 Mal vor, während Alarmobjekt AO_4 in einem Bereich zwischen 90 und 100 Mal vorkommen kann.

G_3 = {
  1000 x AO_1,
  (90, 100) x AO_4,
  (9,11) x AO_5
}

G_4 = {
  1050 x AO_2,
  (75, 85) x AO_4,
  10 x AO_5,
  1 x AO_3
}

[00192] Dabei stellen die Alarmobjekte Repräsentative dar, das heißt, dass nicht notwendigerweise zum Beispiel 1000 Mal der idente Alarmobjekt AO_1 in Alarmobjektgruppe G_3 vorhanden ist, sondern 1000 Alarmobjekte AO vorhanden sind, die ausreichend ähnliche zu Alarmobjekt AO_1 sind, um gemeinsam gezählt zu werden.

[00193] Der erste Schritt, um die Ähnlichkeitsmetrik für große Alarmobjektgruppen G zu berechnen, ist das Finden von Paaren von repräsentativen Alarmobjekten. Aus vorherigen Beispielen ist bekannt, dass Alarmobjekt AO_1 in Alarmobjektgruppe G_3 und Alarmobjekt AO_2 in Alarmobjektgruppe G_4, Alarmobjekt AO_4 in Alarmobjektgruppe G_3 und Alarmobjekt AO_4 in Alarmobjektgruppe G_4, und Alarmobjekt AO_5 in Alarmobjektgruppe G_3 und Alarmobjekt AO_5 in Alarmobjektgruppe G_4 eine Paarung bilden.

[00194] Die jeweiligen Häufigkeiten der Paarungen werden verglichen, indem die Verhältnisse aus der kleineren und größeren Häufigkeit berechnet werden. Sollten Häufigkeiten als Bereiche

angegeben sein, ist die Ähnlichkeit 1, wenn es eine Überschneidung gibt oder der andere Wert innerhalb des Bereichs liegt, andernfalls werden die am nächsten beieinanderliegende Werte der Bereiche für die Verhältnisbildung verwendet.

Paarung AO_1 und AO_2: 1000/1050=0,95
Paarung AO_4 und AO_4: 85/90=0,94
Paarung AO_5 und AO_5: 1,0

[00195] Es existiert keine Paarung für Alarmobjekt AO_3 in Alarmobjektgruppe G_4, die deshalb den Wert 0 zur Gesamtähnlichkeit beiträgt. Die Gesamtähnlichkeit berechnet sich wieder als Durchschnitt der Teilähnlichkeiten, also (0,95+0,94+1,0+0,0)/4 = 0,72. Wie vorhin können Verschiebungen der Reihenfolge herangezogen werden, um die Ähnlichkeit weiter zu verfeinern.

AUSFÜHRUNGSBEISPIEL - AGGREGATIONSMETRIK ZUM ZUSAMMENFASSEN VON ALARMOBJEKTGRUPPEN G

[00196] Im Folgenden wird eine Aggregationsmetrik für Alarmobjektgruppen G erklärt. Die dafür verwendeten Alarmobjektgruppen sind wie folgt.

$G_5 = \{AO_3, AO_4, AO_5, AO_5\}$

$G_6 = \{AO_4, AO_5, AO_3\}$

$G_7 = \{AO_3, AO_3, AO_1\}$

[00197] Wie zu sehen ist, umfasst Alarmobjektgruppe G_5 vier Alarmobjekte AO_3, AO_4, AO_5, AO_5, während Alarmobjektgruppe G_6 und Alarmobjektgruppe G_7 nur jeweils drei Alarmobjekte AO_4, AO_5, AO_3; AO_3, AO_3, AO_1 umfassen. Außerdem kommt Alarmobjekt AO_5 doppelt in Alarmobjektgruppe G_5 und Alarmobjekt AO_3 doppelt in Alarmobjektgruppe G_7 vor.

[00198] Die Alarmobjektgruppenzusammensetzungen wurden beispielhaft so gewählt, um die Aggregationsmetrik zu demonstrieren. In der Praxis wären diese Alarmobjektgruppen G vermutlich zu unähnlich, um sinnvoll zu einem einzigen Alarmobjektmuster P aggregiert zu werden.

[00199] Im Folgenden wird angenommen, dass die Mindestähnlichkeit für Alarmobjekte auf 0,2 festgesetzt wird. Zunächst wird die größte Alarmobjektgruppe G ausgewählt, da diese aufgrund der höheren Anzahl an vorhandenen Alarmobjekten die besten Möglichkeiten für alle anderen Alarmobjektgruppen bietet, gute Paarungen von Alarmobjekten zu finden. Diese Alarmobjektgruppe G ist Alarmobjektgruppe G_5.

[00200] Die erste Alarmobjektgruppe G, die mit dieser repräsentativen Alarmobjektgruppe abgeglichen wird, ist Alarmobjektgruppe G_6. Es werden analog zur Ähnlichkeitsmetrik für kleine Alarmobjektgruppen G, die bestmöglichen Paarungen zwischen den Alarmobjektgruppen G5, G6 gesucht. Diese lauten wie folgt.

AO_3 aus G_5 mit AO_3aus G_6
AO_4 aus G_5 mit AO_4aus G_6
AO_5 aus G_5 mit AO_5aus G_6

[00201] Somit bleibt noch ein Alarmobjekt AO_5 aus Alarmobjektgruppe G_5 übrig, das in keiner Paarung auftritt. Die Paarungen und restlichen nicht-gepaarten Alarmobjekte werden nun in Listen gespeichert, die solange erweitert werden, bis alle Alarmobjektgruppen prozessiert wurden. Dabei stehen die Alarmobjekte AO von Alarmobjektgruppe G_5 an erster Stelle der Listen. Zu diesem Zeitpunkt sehen die Listen wie folgt aus:

(AO_3, AO_3)
(AO_4, AO_4)
(AO_5, AO_5)
(AO_5)

[00202] Es wird nun Alarmobjektgruppe G_7 mit Alarmobjektgruppe G_5 abgeglichen. Dabei entstehen folgende Paarungen:

AO_3 aus G_5 mit AO_3 aus G_7
AO_5 aus G_5 mit AO_3 aus G_7

[00203] Das Paar Alarmobjekt AO_4 aus Alarmobjektgruppe G_5 mit Alarmobjekt AO_3 aus Alarmobjektgruppe G_5 wird nicht gebildet, da es eine geringere Ähnlichkeit als das Paar Alarmobjekt AO_5 aus Alarmobjektgruppe G_5 mit Alarmobjekt AO_3 aus Alarmobjektgruppe G_7 aufweist.

[00204] Es wird kein Paar mit Alarmobjekt AO_1 aus Alarmobjektgruppe G_7 gefunden, da es keine Kombination gibt, die eine Ähnlichkeit ergibt, die über der Mindestähnlichkeit für Alarmobjekte liegt. Somit wird Alarmobjekt AO_1 als eigene Liste zu den aktuellen Listen hinzugefügt. Die erweiterten Listen ergeben sich, indem man die neuen Paarungen zu den jeweiligen Einträgen, die bereits von Alarmobjektgruppe G_5 ausgehend gebildet wurden, hinzufügt. Die Liste ergeben sich somit wie folgt:

(AO_3, AO_3, AO_3)
(AO_4, AO_4)
(AO_5, AO_5, AO_3)
(AO_5)
(AO_1)

[00205] Jede Liste wird nun einzeln mithilfe der zuvor beschriebenen Aggregationsmetrik für Alarmobjekte AO aggregiert. Die resultierenden aggregierten Alarmobjekte werden als Sequenz zu einer neuen Alarmobjektgruppe bzw. einem Alarmobjektmuster P gebildet. Die neue Alarmobjektgruppe lautet also wie folgt.

$G_8 = \{AO_7, AO_8, AO_9, AO_{10}, AO_{11}\}$

[00206] Wobei die Alarmobjekte wie folgt gebildet wurden.

AO_7= {
„A“: <“a1“>,
„B“: <“b1“>,
„C“: <“c1“>,
„D“: <“d1“>
}

AO_8= {
„A“: <“a1“>,
„B“: <“b2“>,
„C“: <“c2“>
}

AO_9= {
„A“: <“a1“>,
„B“: <“b1“>,
„C“: <“c1“, “c3”>,
„D“: <“d1“>
}

AO_{10}= {
„A“: <“a1“>,
„B“: <“b1“>,
„C“: <“c3“>

}

AO_{11}= {
  "A": <"a">,
  "B": <"b1">,
  "C": <["c1", "c2"]>,
  "D": {
    "D1": <"d1">,
    "D2": <"d2">
  },
  "E": <"e2">,
  "F": <"f4">,
  "G": <"g8">
}

Patentansprüche

1. Verfahren zur Klassifizierung von anomalen Betriebszuständen eines Computernetzwerks (1), die auf Variationen unterschiedlicher Angriffstypen zurückzuführen sind,
   - wobei das Computernetzwerk eine Anzahl von Computern umfasst, wobei auf den Computern zumindest ein Angriffserkennungssystem (S_A, S_B) zur Erkennung von anomalen Betriebszuständen des Computers und/oder des Computernetzwerks abläuft, wobei das zumindest eine Angriffserkennungssystem (S_A, S_B) dazu ausgebildet ist, bei Eintreten von anomalen Betriebszuständen, die vorab vorgegebenen Erkennungsfällen entsprechen, insbesondere einen Angriff auf den Computer und/oder das Computernetzwerk darstellen, Alarmobjekte (AO; AO_1, ..., AO_n) zu erstellen, sodass derart eine Alarmobjektsequenz erzeugt wird, in der die einzelnen Alarmobjekte (AO; AO_1, ..., AO_n) in der Abfolge ihres Auftretens, insbesondere versehen mit einem Zeitstempel, enthalten sind,
     wobei den einzelnen Alarmobjekten (AO; AO_1, ..., AO_n) jeweils eine Anzahl von Attributen und den Attributen zugeordneten Werten, insbesondere eine Anzahl von Zahlen, Zeichenketten, Wertelisten, und/oder Objekten, zugeordnet sind, die den jeweils aufgetretenen anomalen Betriebszustand, der als einem Erkennungsfall entsprechend erkannt wurde, charakterisieren,

   dadurch gekennzeichnet,
   - dass die einzelnen Alarmobjekte (AO; AO_1, ..., AO_n) der Alarmobjektsequenz zu Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zusammengefasst werden,
   - dass die einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) basierend auf der Reihenfolge, der Häufigkeit und/oder den Attributen der den jeweiligen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zugeordneten Alarmobjekte (AO; AO_1, ..., AO_n) nach einer vorgegebenen Ähnlichkeitsmetrik hinsichtlich ihrer Ähnlichkeit verglichen und unter Vorgabe eines Alarmobjektgruppen-Ähnlichkeitsschwellenwerts (t) aufgrund deren Ähnlichkeit nach einer vorgegebenen Aggregationsmetrik zu Alarmobjektmustern (P; P_1, ..., P_k) in Form von Datenobjekten zusammengefasst werden,
     wobei den Alarmobjektmustern (P; P_1, ..., P_k) jeweils repräsentative Alarmobjekte (RA; RA_1, ..., P_l) zugewiesen werden, die diejenigen Alarmobjekte (AO; AO_1, ..., AO_n), insbesondere deren Attribute und Werte, die den als ähnlich erkannten Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zugeordnet sind, repräsentieren und wobei jedem Alarmobjektmuster (P; P_1, ..., P_k) ein Angriffstyp zugeordnet wird, und
   - dass diejenigen anomalen Betriebszustände, die denjenigen Alarmobjekten (AO; AO_1, ..., AO_n) zugrunde liegen, die den zu einem jeweiligen Alarmobjektmuster (P; P_1, ..., P_k) zusammengefassten Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zugeordnet sind, als anomale Betriebszustände erkannt werden, die auf denjenigen Angriffstyp zurückzuführen sind, der dem jeweiligen Alarmobjektmuster (P; P_1, ..., P_k) zugeordnet ist.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**,
   - dass die einzelnen Alarmobjekte (AO; AO_1, ..., AO_n) der Alarmsequenz nach der zeitlichen Nähe des Zeitpunkts ihrer Erstellung, insbesondere unter Vorgabe eines zeitlichen Abstandsschwellenwerts (δ), zu Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zusammengefasst werden,
     wobei insbesondere vorgesehen ist, dass eine Anzahl unterschiedlicher zeitlicher Abstandsschwellenwerte (δ_{small}, δ_{large}, δ_3) gleichzeitig für die Zusammenfassung zu Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) herangezogen werden,

   und/oder
   - dass die einzelnen Alarmobjekte (AO; AO_1, ..., AO_n) der Alarmsequenz nach der Ähnlichkeit der den Alarmobjekten (AO; AO_1, ..., AO_n) zugeordneten Attribute zu Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zusammengefasst werden.

3. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass eine Datenbank (D) angelegt wird, wobei in der Datenbank (D) die erstellten Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) und Alarmobjektmuster (P; P_1, ..., P_k), sowie die Zugehörigkeit der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zu den einzelnen Alarmob-

jektmustern (P; P_1, ..., P_k) hinterlegt werden.

4. Verfahren nach Anspruch 3, **dadurch gekennzeichnet**,
- dass die einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) nach deren Erstellung in der Datenbank (D) hinterlegt werden, und
- dass die Alarmobjektmuster (P; P_1, ..., P_k) auf Grundlage der in der Datenbank (D) hinterlegten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) erstellt werden, wobei insbesondere vorgesehen ist, dass, im Fall, dass die Datenbank (D) nur eine einzige Alarmobjektgruppe (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) enthält, ein Alarmobjektmuster (P; P_1, ..., P_k) erstellt wird, dessen repräsentative Alarmobjekte (RA; RA_1, ..., RA_l) den Alarmobjekten (AO; AO_1, ..., AO_n) der einzigen Alarmobjektgruppe (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) entsprechen, insbesondere mit den Alarmobjekten (AO; AO_1, ..., AO_n) der einzigen Alarmobjektgruppe (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) identisch sind.

5. Verfahren nach Anspruch 3 oder 4, **dadurch gekennzeichnet**, dass die Zugehörigkeit der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) zu den einzelnen Alarmobjektmustern in Form von Listen umfassend die einem jeweiligen Alarmobjektmuster zugeordneten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) in der Datenbank hinterlegt wird, wobei Listen zumindest eines der folgenden Typen angelegt werden:
   - unbeschränkte Listen,
   - linear befüllbare Listen,
   - logarithmisch befüllbare Listen, und

   wobei insbesondere vorgesehen ist, dass die Wahrscheinlichkeit einer Ersetzung eines Elements einer logarithmisch befüllbaren Liste mit absteigender Position des Elements in der logarithmisch befüllbaren Liste abnimmt.

6. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass die Ähnlichkeit der Alarmobjekte (AO; AO_1, ..., AO_n) der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) und/oder für neu erstellte Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) die Ähnlichkeit mit den bereits erstellten Alarmobjektmustern (P; P_1, ..., P_k) berechnet wird, indem nach übereinstimmenden Attributen und/oder übereinstimmenden, den Attributen zugeordneten, Werten gesucht wird.

7. Verfahren nach Anspruch 6, **dadurch gekennzeichnet**,
- dass alle Attribute der hinsichtlich ihrer Ähnlichkeit zu analysierenden Alarmobjekte (AO; AO_1, ..., AO_n) miteinander verglichen werden und jeweils die Anzahl der Übereinstimmungen und der Unterschiede der den jeweiligen Attributen zugeordneten Werte ermittelt werden und
- dass eine Gesamtähnlichkeit der Alarmobjekte (AO; AO_1, ..., AO_n) innerhalb einer Alarmobjektgruppe (AO; AO_1, ..., AO_n) als Verhältnis der ermittelten Übereinstimmungen zur Summe der Übereinstimmungen und Unterschiede ermittelt wird.

8. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass die als ähnlich erkannten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) zu Alarmobjektmustern (P; P_1, ..., P_k) zusammengefasst werden, indem
- nach einer vorgegebenen Ähnlichkeitsmetrik nach übereinstimmenden Alarmobjekten (AO; AO_1, ..., AO_n) in den einzelnen als ähnlich erkannten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) gesucht wird, und
- die einzelnen übereinstimmenden Alarmobjekte (AO; AO_1, ..., AO_n) zusammengefasst werden, indem jeweils die als übereinstimmend erkannten Attribute der übereinstimmenden Alarmobjekte (AO; AO_1, ..., AO_n) herangezogen werden und ausgewählte, insbesondere alle, Werte, die den als übereinstimmend erkannten Attributen in den jeweiligen Alarmobjekten (AO; AO_1, ..., AO_n) zugeordnet sind, gemeinsam mit dem jeweiligen Attribut im entsprechenden repräsentativen Alarmobjekt (RA; RA_1, ..., RA_l) des Alarmobjektmusters (P; P_1, ..., P_k) hinterlegt werden.

9. Verfahren nach Anspruch 8, **dadurch gekennzeichnet**, dass beim Zusammenfassen der einzelnen übereinstimmenden Alarmobjekte (AO; AO_1, ..., AO_n) der Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) zu Alarmobjektmustern (P; P_1, ..., P_k)

- Listen umfassend ausgewählte, insbesondere alle, Werte, die einem als übereinstimmend erkannten Attribut in den jeweiligen übereinstimmenden Alarmobjekten (AO; AO_1, ..., AO_n) zugeordnet sind, gemeinsam mit dem jeweiligen Attribut im jeweils entsprechenden repräsentativen Alarmobjekt (RA; RA_1, ..., RA_l) des Alarmobjektmusters (P; P_1, ..., P_k) hinterlegt werden und/oder
- Platzhalter für die Werte, die einem als übereinstimmend erkannten Attribut in den jeweiligen übereinstimmenden Alarmobjekten (AO; AO_1, ..., AO_n) zugeordnet sind, im jeweils entsprechenden repräsentativen Alarmobjekt (RA; RA_1, ..., RA_l) des Alarmobjektmusters (P; P_1, ..., P_k) hinterlegt werden, wenn die Anzahl an unterschiedlichen Werten, die das jeweilige Attribut in den jeweiligen Alarmobjekten annimmt, einen vorgegebenen Maximalwert überschreitet.

10. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass die Ähnlichkeitsmetrik für die Suche nach übereinstimmenden Alarmobjekten (AO; AO_1, ..., AO_n) in den Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) auf zumindest einer der folgenden Vorgehensweisen beruht:
a) dass die den Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zugeordneten Alarmobjekte (AO; AO_1, ..., AO_n) jeweils paarweise hinsichtlich deren Ähnlichkeit miteinander verglichen werden, und dass diejenigen Alarmobjektpaare ermittelt werden, deren Ähnlichkeit am größten ist, wobei insbesondere vorgesehen ist, dass jedes Alarmobjekt (AO; AO_1, ..., AO_n) nur in einem Alarmobjektpaar enthalten ist,
b) dass zunächst innerhalb der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) die Häufigkeiten der einzelnen zugeordneten Alarmobjekte (AO; AO_1, ..., AO_n) ermittelt werden und Alarmobjekte (AO; AO_1, ..., AO_n), deren Ähnlichkeit einen vorgegebenen Alarmobjekt-Ähnlichkeitsschwellenwert übersteigt, als gleich angesehen und zu einem aggregierten Alarmobjekt zusammengefasst werden, dass die aggregierten Alarmobjekte der Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) jeweils paarweise miteinander verglichen werden, und dass diejenigen Alarmobjektpaare ermittelt werden, deren Ähnlichkeit am größten ist, indem die Häufigkeiten der einzelnen zugeordneten Alarmobjekte (AO; AO_1, ..., AO_n) verglichen werden,
c) dass zunächst innerhalb der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) Alarmobjekte (AO; AO_1, ..., AO_n), deren Ähnlichkeit einen vorgegebenen Alarmobjekt-Ähnlichkeitsschwellenwert übersteigt, als gleich angesehen und zu einem aggregierten Alarmobjekt zusammengefasst werden, dass die aggregierten Alarmobjekte der einzelnen Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) Positionen innerhalb des jeweiligen Abschnitts der Alarmsequenz, den die jeweilige Alarmobjektgruppe (G; G_1, ..., G_m; G'_1, ..., G'_m) umfasst, zugeordnet werden und dass mittels Sequenzalignment die Ähnlichkeiten der aggregierten Alarmobjekte der als ähnlich erkannten Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) ermittelt werden.

11. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**, dass das Zusammenfassen der Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) zu Alarmobjektmustern (P; P_1, ..., P_k) nach einer erstmaligen Erkennung neuerlich, insbesondere laufend, durchgeführt wird und die repräsentativen Alarmobjekte (RA; RA_1, ..., RA_l) der einzelnen Alarmobjektmuster (P; P_1, ..., P_k) auf Grundlage der, in den neu hinzugekommenen, als ähnlich erkannten, Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) enthaltenen, Alarmobjekte (AO; AO_1, ..., AO_n), insbesondere mit dem Verfahren eines der Ansprüche 8 bis 10, aktualisiert werden,
wobei insbesondere vorgesehen ist, dass die bereits erstellten Alarmobjektmuster (P; P_1, ..., P_k) mit den neu erstellten Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) mit dem Verfahren eines der Ansprüche 8 bis 10 zusammengefasst werden.

12. Verfahren nach einem der vorangehenden Ansprüche, **dadurch gekennzeichnet**,
- dass für neu erstellte Alarmobjektgruppen (G; G_1, ..., G_m; G'_1, ..., G'_m) die Ähnlichkeit mit den bereits erstellten Alarmobjektmustern (P; P_1, ..., P_k) berechnet wird, wobei eine neue erstellte Alarmobjektgruppe (G; G_1, ..., G_m; G'_1, ..., G'_m) als einem Alarmobjektmuster (P; P_1,

..., P_k) ähnlich erkannt wird, wenn die berechnete Ähnlichkeit zwischen der jeweiligen Alarmobjektgruppe (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) und dem jeweiligen Alarmobjektmuster (P; P_1, ..., P_k) einen vorgegebenen Ähnlichkeitsschwellenwert übersteigt, und

- dass diejenigen Alarmobjektmuster (P; P_1, ..., P_k), denen die neu erstellten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) als ähnlich erkannt wurden, auf Grundlage der, in den neu hinzugekommenen Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) enthaltenen, Alarmobjekte (AO; AO_1, ..., AO_n) aktualisiert, insbesondere die jeweiligen Alarmobjektmuster (P; P_1, ..., P_k) mit den neu erstellten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) mit dem Verfahren eines der Ansprüche 8 bis 11 zusammengefasst, werden,

  wobei, im Fall, dass diejenige Alarmobjektgruppe, die als einem Alarmobjektmuster (P; P_1, ..., P_k) ähnlich erkannt wird, die gleichen Attribute aufweist, wie die Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$), auf denen das jeweilige Alarmobjektmuster (P; P_1, ..., P_k) basiert, die Attribute der repräsentativen Alarmobjekte (RA; RA_1, ..., RA_l) des Alarmobjektmusters (P; P_1, ..., P_k) unverändert bleiben,

und/oder

- dass ein neues Alarmobjektmuster (P; P_1, ..., P_k) erstellt wird, wenn die Ähnlichkeit zwischen den neu erstellten Alarmobjektgruppen (G; G_1, ..., G_m; G‘$_1$, ..., G‘$_m$) und den bereits erstellten Alarmobjektmustern (P; P_1, ..., P_k) den vorgegebenen Ähnlichkeitsschwellenwert nicht übersteigt.

13. Datenträger, auf dem ein Programm zur Durchführung eines Verfahrens nach einem der vorangehenden Ansprüche abgespeichert ist.

Hierzu 5 Blatt Zeichnungen

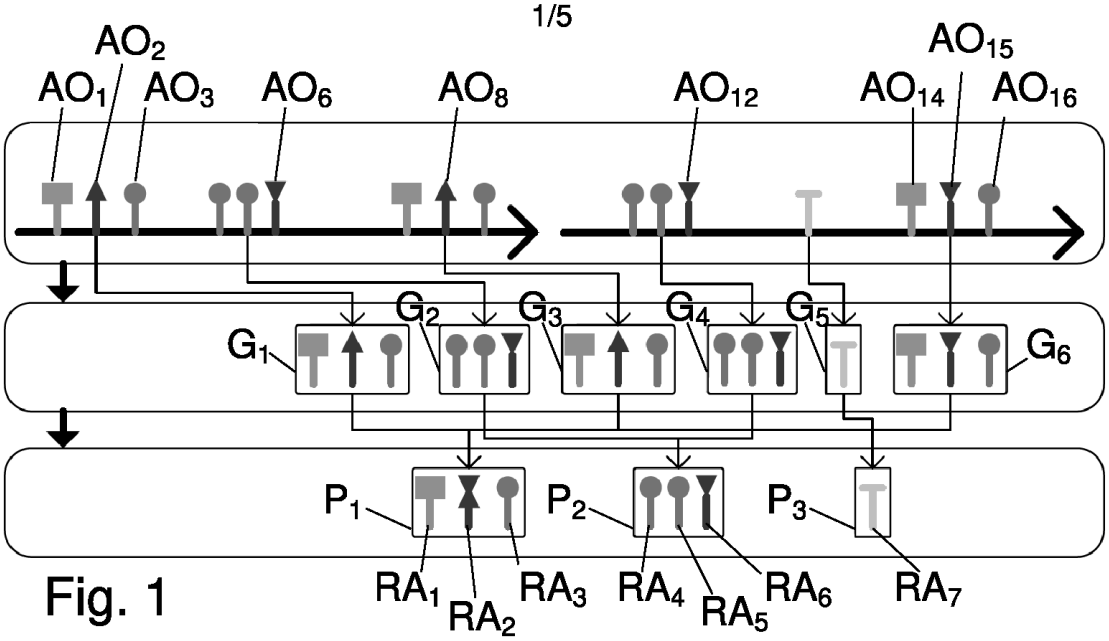


Fig. 1

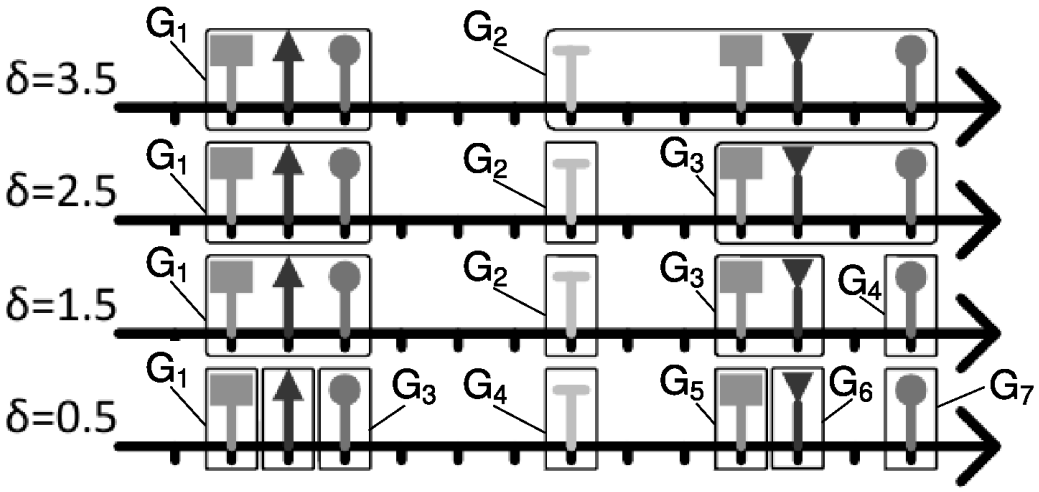


Fig. 2

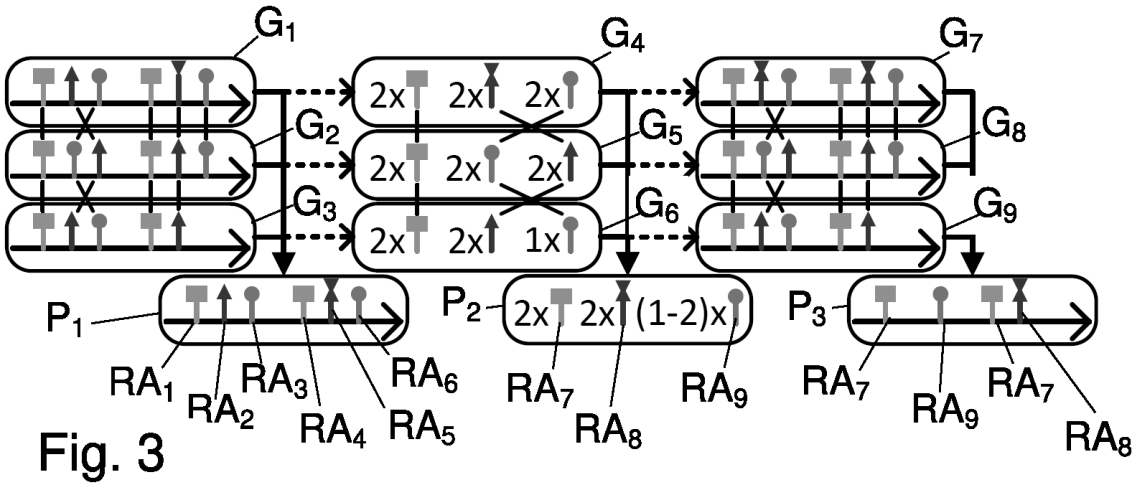


Fig. 3

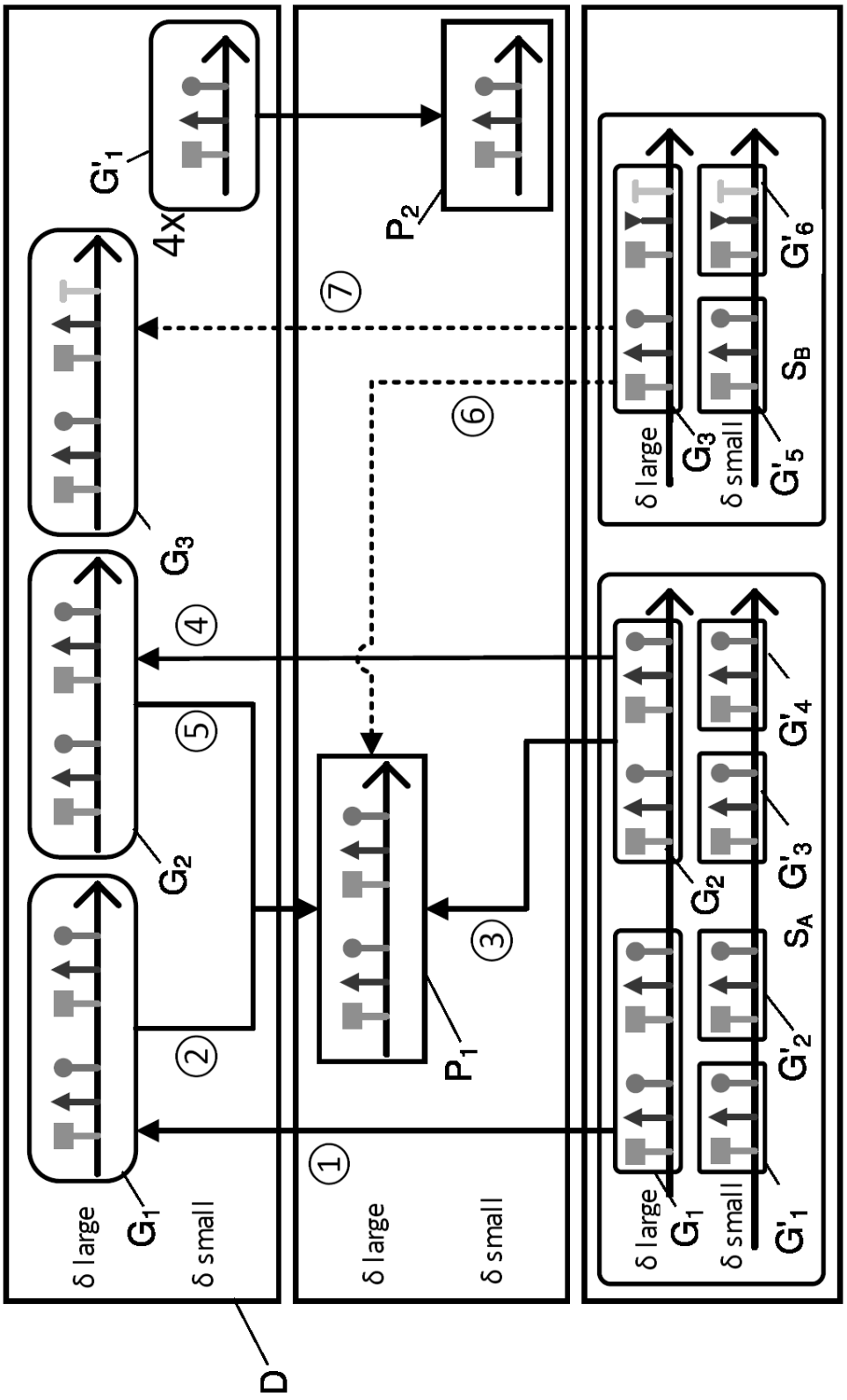


Fig. 4

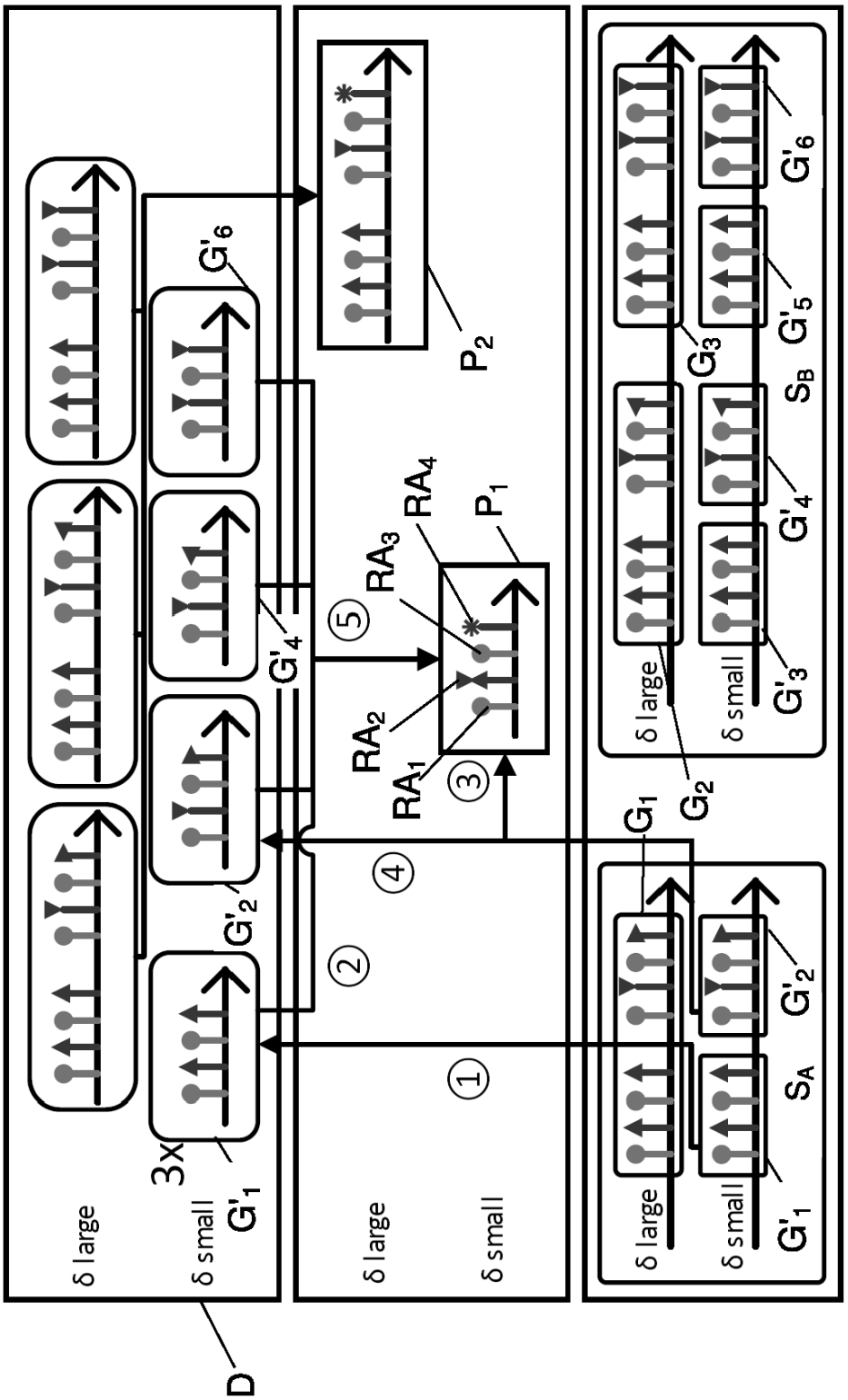

δ large
δ small
3x
G'1
G'2
G'4
G'6
D
①
②
③
④
⑤
RA1
RA2
RA3
RA4
P1
P2
G1
G2
G3
SA
SB
G'3
G'5

Fig. 5

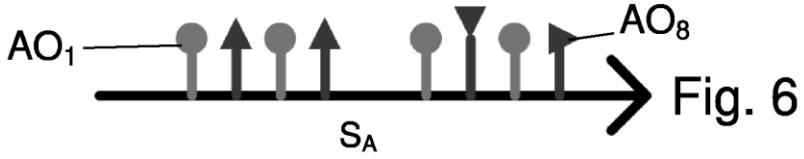


Fig. 6

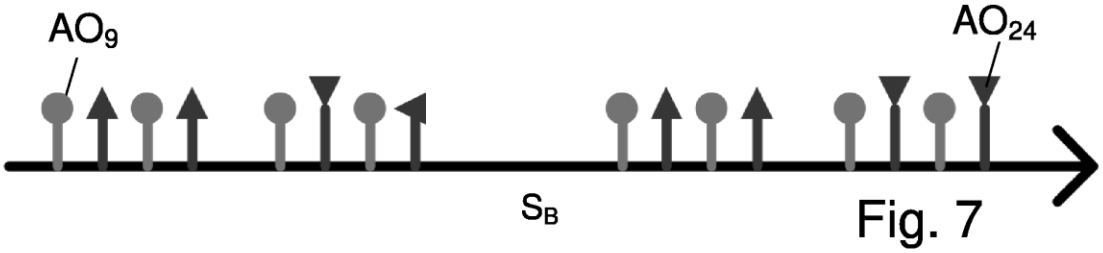


Fig. 7

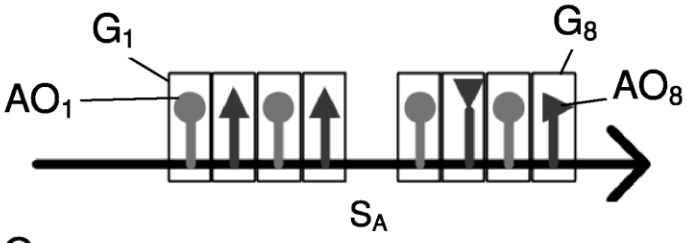
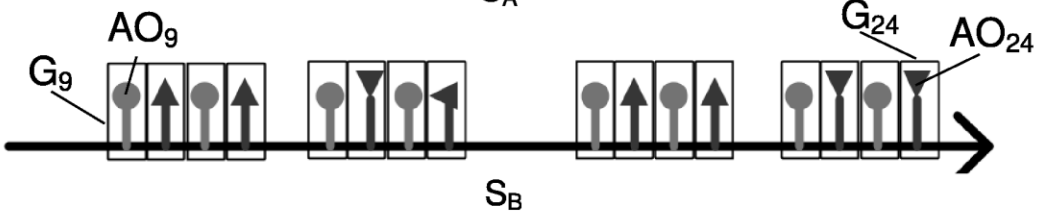


Fig. 8



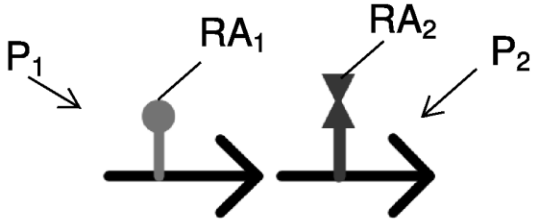


Fig. 9

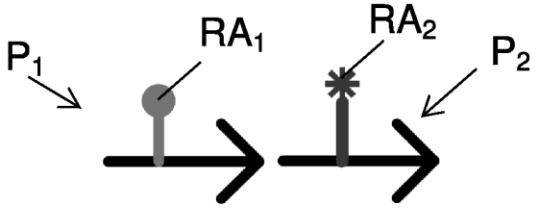


Fig. 10

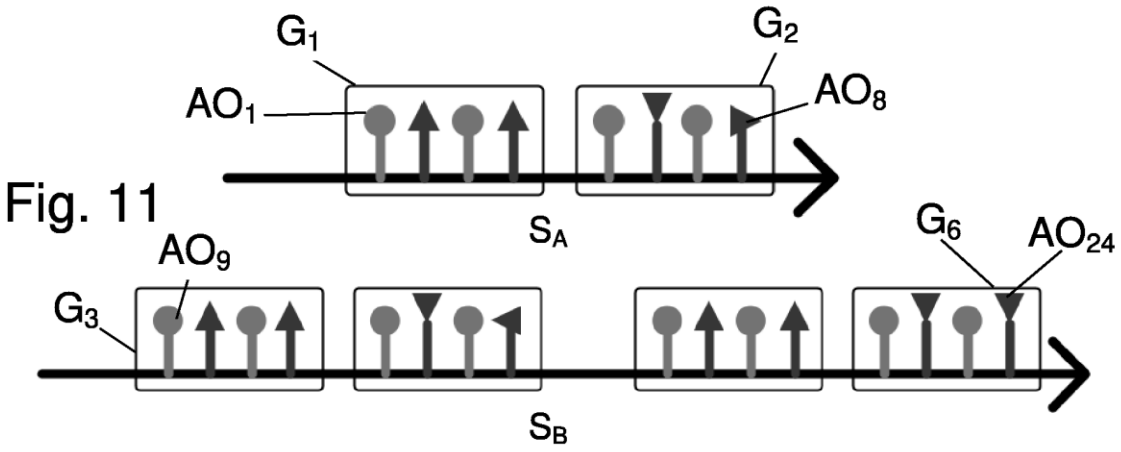


Fig. 11

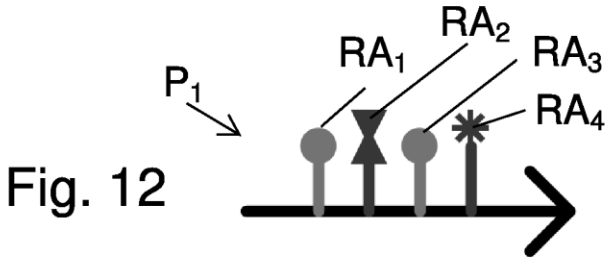


Fig. 12

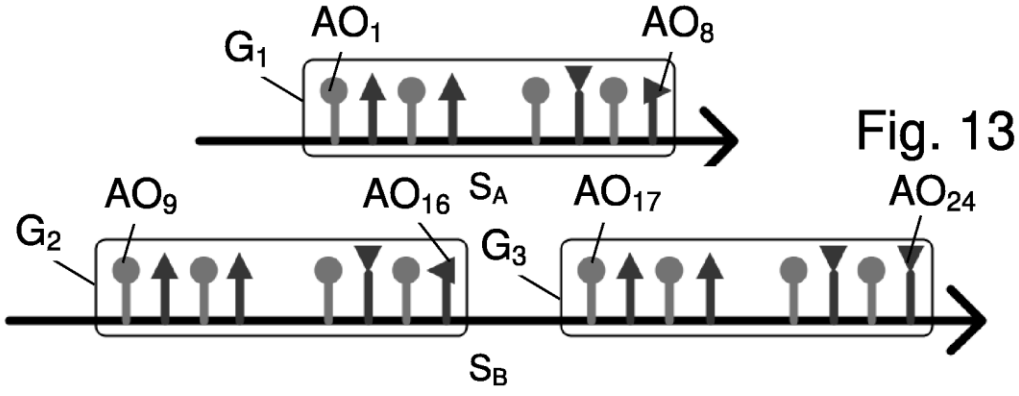


Fig. 13

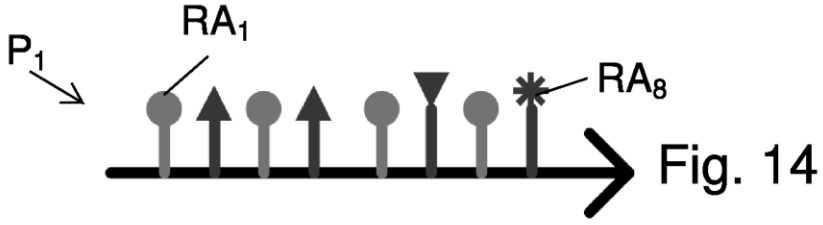


Fig. 14