ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

A Comparative Study of Ids Algorithms on Session Initiation Protocol System

Sinju N Saliya [1], Amruta H Hingmire [2], Ranjini R[3]

Assistant Professor, Department of Computer Engineering, RSCOE, Pune, India[1]

Assistant Professor, Department of Computer Engineering, RSCOE, Pune, India[2]

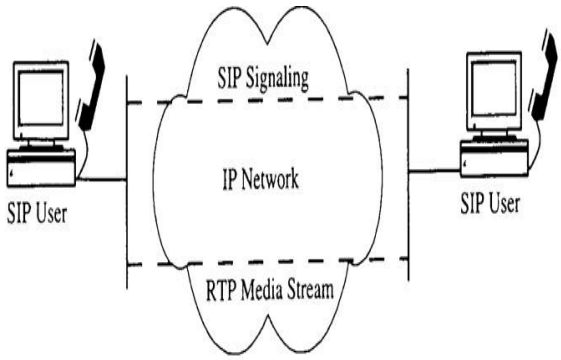
Research Scholar, Department of Computer Engineering, RSCOE, Pune, India [3]

ABSTRACT: Intrusion detection system offer techniques for modeling and recognizing normal and abnormal system behaviour. Session initiation protocol is VoIP standard protocol for create, maintain and end the voice communication. SIP is designed with an open structure due to its openness vulnerable to security attacks. SIP flooding attack is among the most severe attack because it easy to launch and capable of quickly draining the resources of both network and nodes. There have been many detection methods on SIP system. In this paper we present and evaluate various types of IDS algorithms on SIP system.

KEYWORDS: SIP, Anomaly detection, Misuse detection

I. INTRODUCTION

SIP based systems are gaining in popularity as the technology for transmitting voice and video traffic over IP network. SIP is used for many session oriented applications, such as calls, multimedia distributions, video conferencing, and instant messaging. SIP can be used to attack systems[1], denial of service (DoS) attacks are the main concerns causing loss of SIP based systems availability. DoS attacks can consume memory, CPU, and network resources and damage or shut down the operation of the resource under attack (victim)[2]. The aim of a DoS attack is to steal network resources, or to degrade the service perceived by users, where this attack focuses on rendering a network of service unavailable. SIP is an application layer dominated protocol that establishes, modifies and ends multimedia sessions such as conferences. SIP is designed for signalling Multicast call flow, as shown in Figure 1(a).



(a)

There have been many detection methods on SIP flooding attack**,** ie anomaly based detection method or misuse based detection method. Anomaly detection: Attempt to model normal behaviour. Any event which violates this model is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

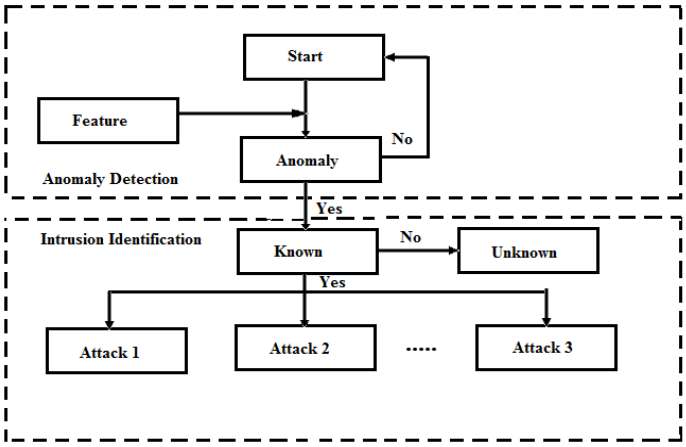
Vol. 6, Issue 1, January 2017

considered to be suspicious. Misuse detection**:** Attempt to model abnormal behaviour, any occurrence of which is clearly indicate of attack, it also known as signature based. Both anomaly based and misused based schemes have their own advantages and disadvantages. Given below table 1(b) shows the comparison of anomaly Vs misuse.

Anomaly Based	Misuse Based
Build a model that represent normal behaviour on the network	Build a model that represent abnormal behaviour on the network
A prior knowledge of the attack is not required and new anomaly unknown before can be detected	Known attack pattern as signature and cannot detect unknown attack
Suffers from accuracy problem(as building an accurate model)	High level of accuracy.
Leading false positive or false negative and gives false alarm	No false positive, and minimum false alarm
Eg:white listing,Hellinger distance	Eg:Pattern matching and honey pots

(b)

The anomaly based approach as shown in Figure 1 (c) builds models that represent normal behaviours on the network.



(c)

Alarms are raised if the observed behaviours significantly deviate from the behaviours estimated by the model. The main advantages of this approach are that a priori knowledge of attack strategy is not required and new anomalies unknown before can be detected. The Anomaly based IDS might come up with several numbers of logs containing numerous network attacks which could possibly be a false positive.

The misuse based approach as shown in Figure 1(d) profiles known attack patterns as signatures. Detection systems in this approach raise alert if the ongoing traffic patterns match the profiled signatures[1]. Misuse based IDS helps in maintaining the integrity of data in a network controlled environment[2]. Unfortunately, this type of IDS depends on predetermined intrusion patterns that are manually created. If the signature database of the Signature based IDS is not updated, network attacks just pass through this type of IDS without being noticed.

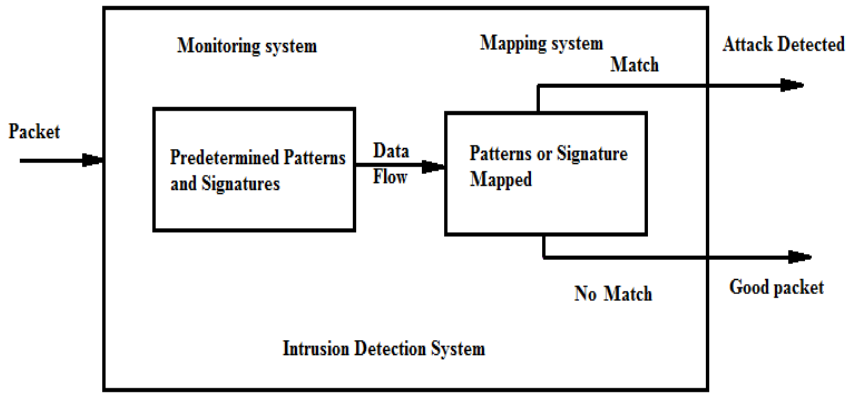
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017



(d)

One big challenge of signature based IDS is that every signature requires an entry in the database, and so a complete database might contain hundreds or even thousands of entries. Each packet is to be compared with all the entries in the database, this can be very resource consuming and doing so will slow down the throughput and making the IDS vulnerable to DoS attacks[3]. Some of the IDS evasion tools use this vulnerability and flood the signature[5]. Signature based IDS systems with too many packets to the point that the IDS cannot keep up with the traffic, thus making the IDS time out and drop packets and as a result, possibly miss attack, this type of IDS is still vulnerable against unknown attacks as it relies on the signatures currently in the database to detect attacks.

II. RELATED WORKS

A. DETECTION OF SIP FLOODING ATTACK BASED ON THE UPPER BOUND OF POSSIBLE NUMBER OF SIP MESSAGES

In this paper they derive an upper bound of the possible number of sip messages, considering not only the network congestion status but also different properties of individual sip messages such as INVITE, BYE and CANCEL. The sip flooding attack detection based on cumulative sum(CUMSUM), Hellinger Distance(HD) and adaptive threshold have two major weak point, they detect sip flooding attack by checking whether the incoming sip messages exceeds certain threshold value[1]. However when a network congestion occur, the number of incoming sip messages may increases because of the retransmission nature of sip messages. and the previous methods detect them as flooding attack even when it is normal condition. second, the previous methods only detect invite flooding attack, they are inefficient in detecting other sip flooding attack such as bye flooding, cancel flooding due to different property of the sip message.

2.1.1 Upper Bound of Possible Number of SIP Messages

The higher the degree of network congestion, the more sip messages that an sip element receives due to retransmission the time is divided into a constant period of Δ, which is a basic unit for traffic measurement. let t_n be the n-th time period and an be the number of newly generated sip messages received at a sip element during t_n where n =0,1,2,....., respectively.
Then the upper bound for possible number of sip messages that the sip element can receive during a given time period is given by

$$m_u^{'} = A\frac{1}{1-P}$$

Where A is the maximum number of sip messages newly generated and received by sip element. P denotes the retransmission due to network congestion. Main advantage of this scheme is considering network congestion and different property of individual sip messages.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

B. UTILIZING BLOOM FILTER FOR DETECTING FLOODING ATTACK AGAINST SIP BASED SERVICES

Bloom filter is a data structure designed to tell you, rapidly and memory efficiently, whether an element is present in a set, false positive matches are possible but false negative are not. Specifically, a set A of elements $(a_1, a_2, a_3, a_4 \cdots\cdots a_n)$ can be stored in the vector V of m bits. All bits of vector V are initially set to zero. To each item of the set hash functions are applied. The hash function results are used as an index to the filter while the value of the corresponding entry is set to one.

2.2.1Detection mechanism (Monitoring system and detection method exist)

The detection mechanism utilizes bloom filter with counters. A two part bloom based monitor has been employed. The main function of monitoring system is to record the state of any incoming session[3]. The first part logs–monitors all new incoming requests, while the second one logs monitors the requests that have been directed to a specific end-user. The detection mechanism considering (a) the average network delay(d_n) and (b) the average user response time (URT).
The session distance is defined by,

$$dist = Num\ of\ INVITES - 05 * (Num\ of\ OK + Num\ of\ ACK)$$

In a well behaved environment the session distance metric for any established session is equal to zero. The required time to detect the attack is negligible, When a network congestion occur the normal traffic will increase. Which gives false positive and leads to false alarm.

C. DETECTION OF INTRUDERS AND FLOODING IN VOIP USING IDS, JACOBSON FAST AND HELLINGER DISTANCE ALGORITHM

The VFDS (VoIP flooding detection system) detect anomalies in collection of packet streams, going through a cyclic behaviour consisting of two phases: the training phase and testing phase. [8]Using Hellinger distance (HD) calculate the probabilistic distribution of training data, the probabilistic distribution of testing data and the threshold of deviation (to distinguish normal behaviour from the abnormal behaviour)
Hellinger Distance

Hellinger distance is used to find the deviation between two probability distribution. let P and Q be two probability distribution on a finite sample space Ω where P and Q are n tuples $(p_1, p_2, p_3 \cdots\cdots p_n)$ and $(q_1, q_2, q_3 \cdots\cdots q_n)$ then the HD between P and Q is defined by

$$D_h^2(p,q) = \frac{1}{2}\sum_{i=1}^{i=n}\left(\sqrt{p} + \sqrt{q}\right)^2 \ (D_h^2 = 0\ when\ p = q)$$

HD can also be used to measuring protocol deviations. In an anomaly based detection mechanism we need to design normal traffic behaviour. To accurately track of normal behaviour, use a dynamic threshold for detection. the threshold is an instance of Jacobson's fast algorithm. This mechanism work for low traffic and highly congested traffic and avoid false alarm.

D. SIP FLOODING ATTACK DETECTION WITH A MULTIDIMENSIONAL SKETCH DESIGN

The system operation is based on two techniques, sketch and hellinger distance, the sketch data structure is probabilistic data summarization techniques. Sketch able to derive a constant-size traffic summary[9]. The hellinger distance (HD) is used to measure the distance between two probability distributions. The HD between two distributions is defined as follows,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

$$D^2(p,q) = \frac{1}{2}\sum_{i=1}^{n}\left(\sqrt{p_i} - \sqrt{q_i}\right)^2$$

Where $p = (p_1, p_2, p_3, \cdots p_n)$ and q = $(q_1, q_2, q_3, \cdots q_n)$
A low HD value implies that there is no significant deviation in the current traffic observations and a high HD is a strong indication that anomalies have happened. Hence HD can reflect Current traffic behaviour along time,

2.4.1 Detection Threshold

A detection threshold is needed to reflect the normal condition and the actual indicator of anomalies. The threshold value computed using Exponential weighted moving average(EWMA)
Estimated threshold is given by

$$H_{n+1}^{thr} = \boldsymbol{\lambda} \cdot H_n + \mu \cdot S_n$$
$$H_n = (1-\alpha) \cdot H_{n-1} + \alpha \cdot H_n$$
$$S_n = (1-\beta) \cdot S_{n-1} + \beta \cdot |H_n - h_n|$$

Where H_n is the estimation average of h_n (h_n is the value of HD in the current time interval n) and S_n be the current mean deviation. The detection scheme is fully effective in multi-attribute attack and is able to discriminate different form of sip flooding .It preserve high accuracy but some time may gives false alarm and are not able to effectively address stealthy flooding attack.

E. CHANGE POINT MONITORING FOR THE DETECTION OF DOS ATTACKS

The objective of change point detection is to determine if the observed time series is statistically homogeneous and if not, to find the point in time when the change happens. It based on the inherent network protocol behaviours. There exist mainly two type of test for different problems, They are posterior test and sequential test, the posterior test are done offline, where entire data collected first and then a decision of homogeneity or a change point is made based on the analysis of all the collected data. Similarly the sequential test are done online with the data presented sequentially, and the decision are made on the fly. It has quick response, save memory and computation. Cumulative sum algorithm is a change point detection algorithm. which belongs to the category of sequential test[10]. cusum is a non parametric and stateless method. It can detect anomalies from the network based on inherent network protocol behaviours. Let $\Delta_n (n = 0,1,2 \ldots \ldots n)$ be the number of request minus that of corresponding replays collected within one sampling period. R' denotes the average number of replays, then $X_n = {}^{\Delta_n}/_{R'}$ where X_n is a stationary random process under normal condition the mean of X_n denoted as c.

$$X_n = X_n - a \text{ (“a” is an upper bound of c)}$$

The above expression have negative mean during normal operation. when DOS attack take place , X_n will suddenly increases and become a large positive number. The technique is very robust, generally applicable and deployment in much easier.

F. HONEYCOMB-CREATING INTRUSION DETECTION SIGNATURES USING HONEYPOTS

The system that generates signatures for malicious network traffic automatically, pattern matching technique and protocol conformance checks are applied. The system is unique. It cannot read a database of signatures upon start-up to match then against live traffic to spot matches. The system tries to spot pattern in the traffic previously seen on the honey pot. It uses longest common substring (LCS) algorithm to spot similarities in packet payloads, the LCS implementation is based on suffix tree. Each received packet causes honeycomb to initiate certain sequence of activities. Honeycomb maintains state for limited number of TCP and UDP connections. Generating signature by comparing new traffic on the honey pot to previously seen one, the signature record has unique identifier and stored discovered facts about the currently investigated traffic, if a common substring is found that exceeds a configurable minimum length, the substring is added to the signature as a new payload byte pattern. The system produces good quality signatures on a typical end users internet connection.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

G. AUTOMATED SIGNATURE CREATOR FOR A SIGNATURE BASED INTRUSION DETECTION SYSTEM WITH NETWORK ATTACK DETECTION CAPABILITY (PANCAKE)

Pancake is an automated signature creator, solution for the manual signature creation. Through this system, signature will be created automatically. Before pancake can generate signature a module called log attribute selected module is implemented[11]. Pancake will generate signature that is to be passed on and fed to the signature based IDS, The signature are generated based on non payload based detection rule. Logs and the packet captures would be the basis of the signature generation. Automation of signature is possible with the use of machine learning. Through machine learning, the system was able to further determine the malicious instances within a capture file that is already pre analysed by an anomaly based IDS.

H. NOVEL ALGORITHM FOR INTRUSION DETECTION SYSTEM

The technique is based on the signature based intrusion detection. Intrusion can be possible at the header part or payload part. String matching algorithm is used analyse the network traffic. The algorithm is used to reduce the false alarm count, if pattern is repeated more than two times that it will be intrusion instead of normal data. In such a cases the alarm will triggered. Time complexity of LFA algorithm is O(n),number of comparison O(n) and in worse case $O(n + m)$reduce false alarm percentage.

I. DYNAMIC MULTILAYER SIGNATURE BASED INTRUSION DETECTION SYSTEM USING MOBILE AGENT

Dynamic multilayer model The model consist of multiple intrusion detection system deployed in different layer and each one contained with small signature data base. The smaller database contain the most frequent attack signature, and a bigger complementary signature data base containing thousands of signature used to update smaller data base from time to time using mobile agent[12]. Mobile Agent are used to performing the updating process of small signature database. Main aim of the system is to improve the throughput of signature based ids[14]. Main parameters are MinFreq (minimum number of attack occurrence to be considered as frequent),ValidTime (Time beyond which the attack seen are considered as valid and threatening) MaxNum(representing maximum number of the signature acceptable in all ids)

J. NOVEL DOS/DDOS ATTACK DETECTION AND SIGNATURE GENERATION

The main function of the system is to detecting the novel attack in real time without human involvement and generate signature of novel attack in real time without human involvement The signature based IDPS prevent the server from known DOS/DDOS attack. Anomaly detection based filter and signature generator are used to generate signature, which can represent novel attack[13]. Known attack signature DB (KASDB) contain signature of known attacks, and used by signature based ids to detect them.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

III. EXPERIMENTAL RESULTS

The given below table 3(a) compare various type of IDS algorithm. The parameter used for comparison are false alarm rate and response rate.

Sno	Title	Anomaly/Misuse	Detection algorithm	FalselAarm	Rapid Response	Advantage
1	Detection Of SIP Flooding Attack Based On The Upper Bound Of Possible Number Of SIP Messages	Anomaly	Upper bound mechanism	No	Yes	Considering network congestion
2	Utilizing Bloom Filter For Detecting Flooding Attack Against SIP Based Services	Anomaly	Bloom filter based monitoring	Yes	Yes	Time to detect attack is negligible
3	Detection Of Intruders And Flooding InVOIP UsingIDS, Jacobson Fast And Hellinger distance algorithm	Anomaly	Jacobson fast and Hellinger distance algorithm	yes	Yes	Can detect unknown attack, high detection accuracy
4	Sip Flooding Attack Detection With a Multidimensional Sketch Design	Anomaly	Hellinger distance algorithm	yes	Yes	Robust, can detect multi attribute attack
5	Change Point Monitoring For The Detection Of DOS Attacks	Anomlay	Cummulative sum algorithm	yes	Yes	Robust, generally applicable, deployment is much easier
6	Honeycomb-Creating Intrusion Detection Signatures Using Honeypots	Misuse	Pattern detection technique (Longest common substring algorithm)	No	No	High detection accuracy
7	Automated Signature Creator For a Signature Based Intrusion Detection System With network Attack Detection Capability(Pancake)	Misuse	Machine learning technique	No	No	Automatic signature can detect unknown attack
8	Novel Algorithm For Intrusion Detection System	Misuse	Less false alarm algorithm	No	No	Reduce false alarming
9	Dynamic Multilayer Signature Based Intrusion Detection System Using Mobile Agent	misuse	Algorithm using mobile agent	No	No	Improved throughput

(a)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

IV. CONCLUSION

On The survey existing SIP flooding detection schemes are either anomaly based or misuse based. The anomaly based detection scheme uses Hellinger Distance algorithm (HD), Cumulative SUM algorithm (CUSUM), adaptive threshold algorithm, etc to detect anomaly. The anomaly based scheme can detect unknown attack it does not need the prior knowledge of the attack, but it generates some false alarm, suffers from accuracy problem and gives false positive. Similarly the misuse based scheme uses Weighted SUM algorithm (WSUM), Expression matching method, Honeypot for the detection. These algorithms have high detection accuracy, no false positive but it cannot detect unknown attack. To overcome problems in both SIP flooding detection schemes a hybrid detection scheme is proposed. The proposed hybrid scheme consist features of both anomaly based scheme and misuse based scheme and it gives fast response, increase accuracy of detection and no false alarm.

In propose combine the advantage of both anomaly and misuse based detection, and an improved security-enhanced SIP System to reduce effect of SIP flooding attacks. This mechanism include components from both anomaly and misuse based system hence it gives a hybrid detection mechanism with high detection accuracy, fast response and no false alarm.

REFERENCES

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, " SIP:Session Initiation Protocol", *RFC 3261, IETF Network Working Group, 2002*

[2] H. Schulzrinne, S. Narayanan, J. Lennox, and M. Doyle, "SIPstone- benchmarking SIP server performance", Technical *Report, Department ofComputer Science, Columbia University, New York, 2002*.

[3] H. Wang, D. Zhang, and K. Shin, "Change-Point Monitoring for the Detection of DoS Attacks", *IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 4, Oct.-Dec., 2004*.

[4] E. Chen, "Detecting DoS attacks on SIP systems," *in 1st IEEE Workshop on VoIP Management and Security, P 53– 58, 2006.*

[5] Husam Al-Alouni, "An Intrusion Detection Approach to Computer Networks", *master of science thesis, military technical college, Cairo, 2003.*

[6] Vijay Katkar S. G. Bhirud," Novel DoS/DDoS Attack Detection and Signature Generation", *International Journal of Computer Applications (0975 – 888),Volume 47– No.10, June 2012*

[7] Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents" .*International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.*

[8] Lata, Kashyap Indu," Novel Algorithm for Intrusion Detection System", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013

[9] H. Sengar, D. Wijesekera, H. Wang and S. Jajodia, "VoIP Intrusion Detection Through Interacting Protocol State Machines," *Proc. IEEE International Conference on Dependable Systems and Networks,2006*

[10] E. Chen, "Detecting DoS Attacks on SIP Systems," *Proc. 1st IEEE Workshop on VoIP Management and Security, 2006.*

[11] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of Service Attacks Targeting a SIP VoIP Infrastructure: Attack Scenarios and Prevention Mechanisms," *IEEE Network*, vol. 20, no. 5, pp. 26-31, Sept.-Oct.2006.

[12] J. Tang, Y. Cheng and Y. Hao, "Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks," *Proc. IEEE INFOCOM, 2012*

[13] Husam Al-Alouni, "security of voice over internet protocol", *PhD of science thesis, military technical college, Cairo, 2010.*

[14] Xianglin Deng and Malcolm Shore, "Advanced Flooding Attack on a SIP Server", *In Proceedings of the The Forth International Conference on Availability, Reliability and Security, Fukuoka, Japan, March 2009*.

[15] B. Rozovskii, A. Tartakovsky, R. Bla˘zek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods", *IEEE Transactions on Signal Processing, 2006.*