The Research of Data Stream Technology in Computer Network Security Monitoring

LI Li [1, a], HU ZhiYu [2]

[1,2] JINGDEZHEN UNIVERSITY, JiangXi JINGDEZHEN 333000,China

[a]lili2015@126.com

Keywords: Network Security Monitoring, Data Stream, Network Event

Abstract: Network attack in a wide range of complex and require monitoring system can real-time detection under high-speed network traffic found various security events. Data stream management system is a kind of high speed and large flow data stream of the real-time response to query requests database model. In this paper, the flow of data in computer network security monitoring technology carried out research. Data stream management platform effectively support real-time query and analysis of the high-speed network data flow, and based on the network security event monitoring system can achieve high processing performance. Put forward a data stream technique is applied to the network security event monitoring framework model can accurately describe the security event in the rules and various monitoring queries, strong flexibility and integrity. In addition, the system can integrate intrusion detection, worms found, network traffic management and so on a variety of monitoring capability, has a good scalability.

Introduction

Network security event monitoring includes all kinds of large-scale worm, such as port scanning, DOS attack, such as security incidents of real-time monitoring and discovery. The traditional solution is to use intrusion detection technology (including misuse detection and anomaly detection, etc.), combined with all kinds of worm found and network traffic analysis method, complete security incident alarm and prevention. The development of the Internet to implement efficient worldwide provides convenient resources and information sharing, and also puts forward new challenges to network security and intrusion detection system. Increasingly complex network system structure, widely used in the distributed application environment, mass storage and high bandwidth transmission technology, makes the traditional intrusion detection becomes more and more cannot satisfy the security requirements of the system [1]. In this case, we need from many aspects, such as system model, architecture, implementation technology and implement new intrusion detection method is put forward, to adapt to the increasingly complex network security event monitoring requirements [2].

Data stream management platform by using the continuous queries and sliding window model, supporting real-time query and analysis of the high-speed network data flow. Based on the data stream management platform of network security event monitoring system has accurate, concise and complete interface language and powerful expression ability, can integrate various network attack detection based on the rules of IDS, worms, found that network status monitoring, and other functions, has a good scalability.

Overview of data stream technology

Database technology in the past few decades was a brilliant success, and has produced many successful system and application, to a great extent, changed the way people work and life. But at the end of the 20th century, appear in some new applications, a new data type, with a powerful challenge to the traditional database technology. This new application mode called the data stream model, the typical application scenarios include: network monitoring and traffic control, sensor network, telephone communication record, financial transactions, web log and click on the flow and so on [3]. The abstract model of the data stream processing is shown in figure 1 is available. System is to maintain a much smaller than the original data in the memory size of structure, known as the "summary data structure", to reflect the characteristics of the original data. The new data arrives, the old data fails, will continue to change the contents of the summary data structure; And at any time, user can meet the precision requirement is obtained by profile data structure of the query results [4].

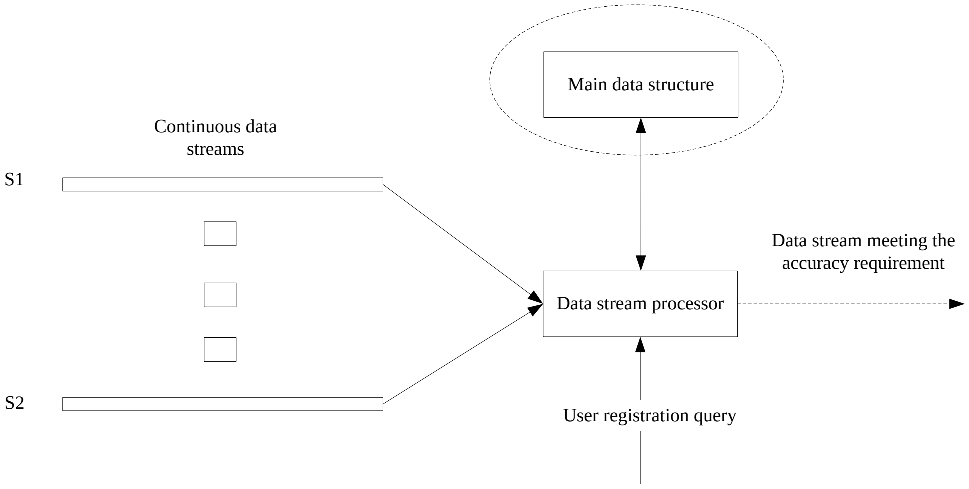

Figure 1. Abstract model of data stream processing

To handle this model using the traditional technology, all data must be stored in the medium, and then by submitting a DML statement access storage medium to obtain the query results. But, due to the large scale data and arrive quickly, the traditional technology in computing storage overhead, continuous real-time tracking results is difficult to meet the practical requirements. Network security monitoring is a typical data stream scenarios. So this article mainly USES the data stream technology to solve some problems in network security monitoring. This section first introduces the related project overview of the data stream management system at home and abroad, then analyses the data stream processing technology research status and development trend in the field of network monitoring.

The overall structural design for Network security event monitoring

Security event monitoring system includes monitoring subsystem, control subsystem, management platform subsystem and safety event store four subsystems. Extracted from monitoring subsystem, the management platform subsystem configuration parameters and operating command, network original data was obtained from the extended router or flow statistics, provide relevant safety event information control subsystem and decision-making basis, safety and operation log write security events library; Control subsystem configuration parameters and operating command was obtained from the management platform subsystem, relevant security event information was obtained from the monitoring subsystem and decision-making basis, to extend the router sends the control command, control operation log write safety event library; Management platform subsystem monitoring subsystem and control subsystem configuration parameters and operating command, library to get the data from security events; Security event repository storage management platform subsystem, monitoring subsystem and control subsystem of various data, provide data to management platform subsystem [5]. Relationship between the general structure of the monitoring system of security events such as the above said, its general structure design is shown in figure 2.

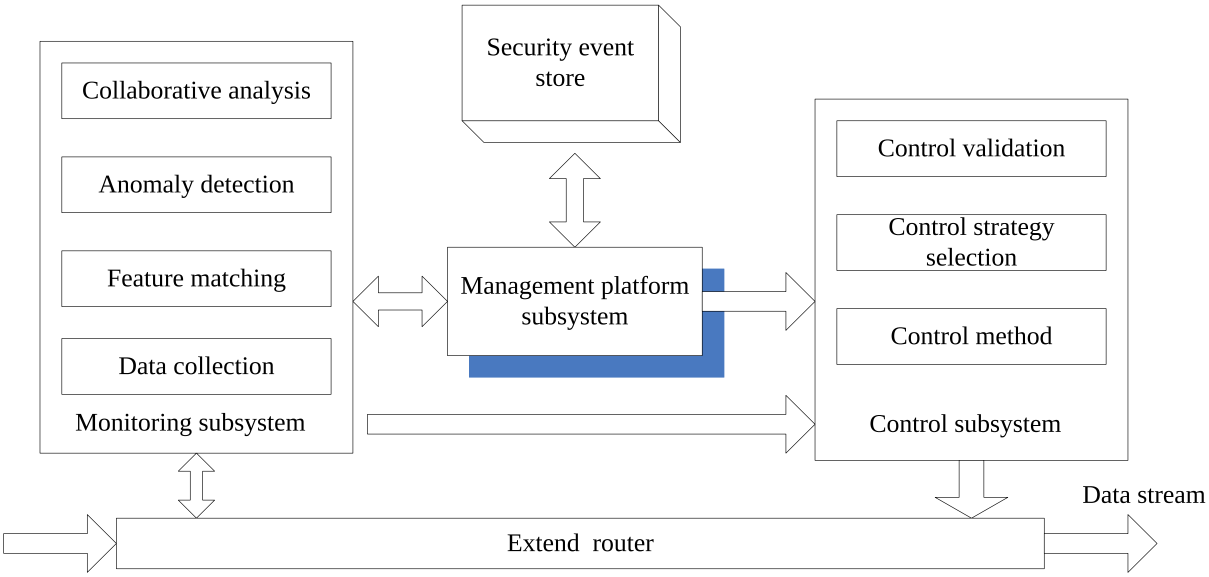

Figure 2. The overall structure of network security event monitoring

Network security event monitoring system design based on data stream processing model

Model based on data Stream processing network security event monitoring system includes three modules: network data preprocessing module, query engine module, user interaction module (user submit a query and result feedback), the structure of the system is shown in figure 3. The system input data source is distributed across multiple patch network Packet detector, collected by means of Packet capture network packets. The original network Packet Flow pretreatment, form conforms to the format of the data Stream. Predefined 3 Flow: Packet - Stream, Keyword - Stream and Flow - the Stream.

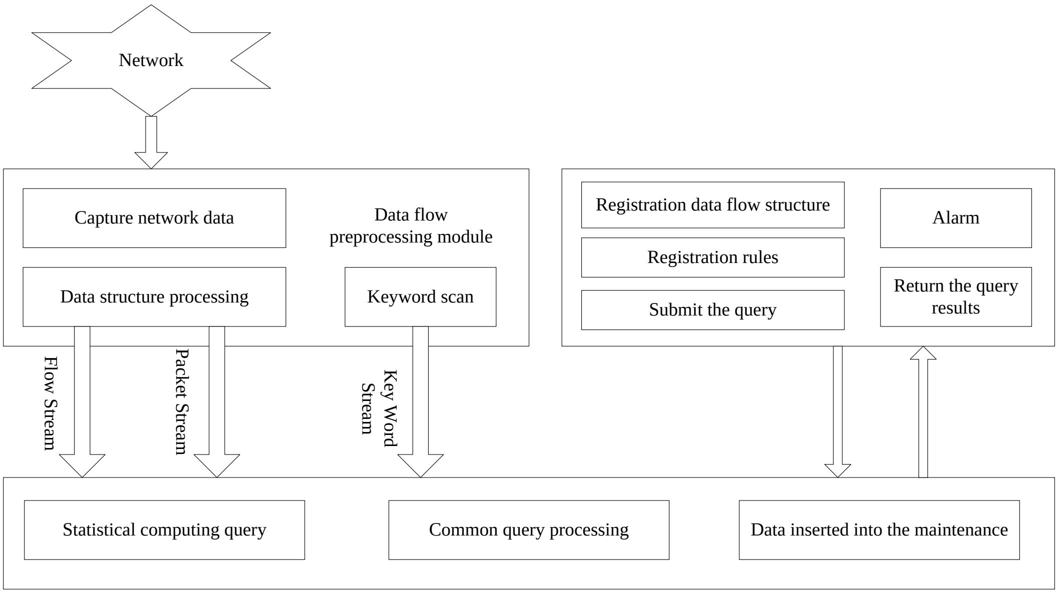

Figure 3. Network security event monitoring system based on data stream processing model

Through this article 3 flow, can complete most of the network security event monitoring function. The specific format specification in the back of the data preprocessing module is discussed. If the user need other application-specific flow, can be registered according to the corresponding flow format. A variety of monitoring requirements are using continuous queries of CQL language writing, such as intrusion detection rules for similar IDS attacks statements, worm detection rule statements, as well as corresponding to various related network monitoring statistics, and other statements. The system will continue to query function continuous data streams, the arrival of continuously produce the query results in the form of continuous flow. The query results are forwarded to the real time a trigger module, alarm to detect intrusion behavior, can also be cached in system, when need to submit the user to see.

Conclusion

Security many applications show the typical data stream applications, especially network security event monitoring and analysis system. The security applications must be continuous without delay handling online, continuous high-speed network data flow, and the network data cannot be stored in external memory. All of our research is based on the continuous query model and the sliding window technology, using data stream management system as stream data processing platform, apply it to the network security monitoring system, implemented a model based on data stream processing network security event monitoring system. In this system, data stream management platform by optimizing execution registered in the system, a large number of continuous queries, to filter, continuous flow network connection, gathered, such as operation, complete the various security event monitoring and alarm, thereby effectively support the real-time monitoring and control system, the flexibility and accuracy requirements.

References

[1] Wood A, Stankovic J A, Virone G: Network, IEEE, 2008, 22(4): 26-33.

[2] Enck W, Gilbert P, Chun B G: Communications of the ACM, 2014, 57(3): 99-106.

[3] Fischer F, Mansmann F, Keim D A, et al. Large-scale network monitoring for visual analysis of attacks[M]. Springer Berlin Heidelberg, 2008.

[4] Aydın M A, Zaim A H, Ceylan K G: Computers & Electrical Engineering, 2009, 35(3): 517-526.

[5] Karim Ganame A, Bourgeois J, Bidou R: computers & security, 2008, 27(1): 30-47.