Software defined network intrusion detection in wireless sensor network

Nan Yan[a], Ping Zhang

School of Computer and Information, Anhui Polytechnic University, 241000 Wuhu, China

Abstract: Software Defined Network (SDN) realizes the separation of control functions from data planes and network programming. It lays the foundation for centralized and refined control and has greater advantages over traditional networks. At present, the research on SDN mainly focuses on wired network and data center, while software definition is proposed in some studies, but only in the stages of models and concepts. According to the characteristics of wireless sensor networks, this paper takes anomaly intrusion detection as the main research content. The sensor network is defined based on OpenFlow software combined with SDN, and intrusion detection technology is studies on the basis of this. It is easier for the system to control the network and its resources in SDN architecture. The Network traffic shows self-similarity in large time scale. In this paper, it can distinguish between the normal situation and the attack by observing the change of the self-similarity coefficient of the network, so as to realize the intrusion detection.

1 Introduction

At present, a lot of research on WSN have conducted by many organizations and research institutions at home and abroad. But the field of WSN security is still in its infancy [1]. As an active and real-time prevention strategy, WSN intrusion detection technology is one of the research areas that researchers focus on. The traditional intrusion method is divided into three levels: 1) Physical layer intrusion is mainly divided into physical damage and congestion attack. 2) The data link layer has energy exhaustion attacks and collision attacks. 3) The attacks on the network layer is most diverse. Due to the fixed routing protocols, traditional wireless sensor networks are vulnerable to intrusion according to the characteristics of each protocol.

Le et al. proposed a WSN intrusion prevention and detection scheme based on clustering structure. In the intrusion detection scheme, a symmetric encryption protocol is adopted to ensure the authenticity of data source identity and the security of communication. Sink nodes monitor the possible attacks within its monitoring area by a series of rules, and notify each node by broadcasting after discovering the attacks. According to the experimental results, their scheme has a higher detection rate for a certain number of attacks such as hello attack, flood attack, data falsification attack and blocking attack. However, the synchronization of these two protocols will result in higher communication and computational overhead, which increases the energy consumption of the nodes and reduces the lifetime of the whole network. Su.Wei-Tsung et al. proposed a LEACH protocol-based security and energy-saving mechanism which is called eHIP detection. The authenticity of control information and monitoring data in ensured by authentication algorithm in this mechanism. At the same time, a cooperative detection algorithm is proposed to ensure security through mutual supervision mechanism between cluster head nodes and cluster member nodes. According to the simulation results, their scheme can effectively save energy in the wake-up mode, but the mechanism can only detect a limited attack line. Abduvaliyev et al. used a bionics algorithm to detect and locate network intruders [4]. Their algorithm is to use bio-simulation algorithms to detect and expel intruders at the edge of the network, just as the respiratory system of an organism has the same sneezing reaction to the foreign body entering the nose. Each sensor node has its own identifier and a whitelist of legitimate nodes, and the abnormal nodes are discovered by mutual monitoring. This release mechanism is essentially based on signature traffic monitoring technology and is an abnormal detection, but the scheme only focuses on unauthorized node intrusion behavior.

At present, there are many SDN-based network security studies. For example, the OpenFlow switch is connected to the downstream direction of the boundary router. The traffic first passes through the boundary, then passes through the OpenFlow switch. Finally, forwarding according to the original path. When the traffic passes through the OpenFlow switch, the attack traffic will be blocked and malicious traffic sample will be collected by operating the OpenFlow switch forwarding table [2]. The Header Space Analysis (HSA) for network state detection and modeling and protocol-independent is proposed by Stanford University in 2012. It mainly used to help network administrators to static analysis of network status, detect the network failures and protection of traffic isolation between different users, etc. The idea of HSA was originally derived from a paper published by Mohammad

[a]Corresponding author: 16417442@qq.com

Al-Fares at SIGCOMM in 2008[6]. This paper proposes the idea of classify data packets by multidimensional geometry. In 2013, a real-time policy detection tool based on HAS for SDN networks is proposed in a laboratory at Stanford University. This tool can detect network faults in real time and solve the reachability and loop problems of SDN network [3].

In this paper, the OpenFlow technology of SDN is used to separate network control and data transmission. In the management and control level, the control level of all devices in the network is virtualized to deal with routing switching, protocol processing and so on. In the data level, all the forwarded packets are encapsulated [5]. The specific path and forwarding strategy are calculated and selected by the control protocol, and the whole forwarding process is invisible to the outside world. The OpenFlow architecture consists of two main components: OpenFlow switches, streams, and controllers. In an OpenFlow network, the OpenFlow switch is only responsible for forwarding data streams in the network. The logical control of the whole network is completely under the responsibility of the controller. There is a secure channel between the controller and the OpenFlow switch is responsible for communication.

2 The intrusion detection design of software-defined wireless sensor network

2.1 Network architecture

In the new intrusion detection scheme which is based on software define sensor network architecture, the core part includes two layers of intrusion detection system. The first layer is the Centernode intrusion detection module. The Centernode is responsible for the detection and analysis of the logical subnets. The other layer is the Masternode analysis control module which analysis the intrusion according to WSN network log information and logical subnet node information. The overall structure of the system is as follows:

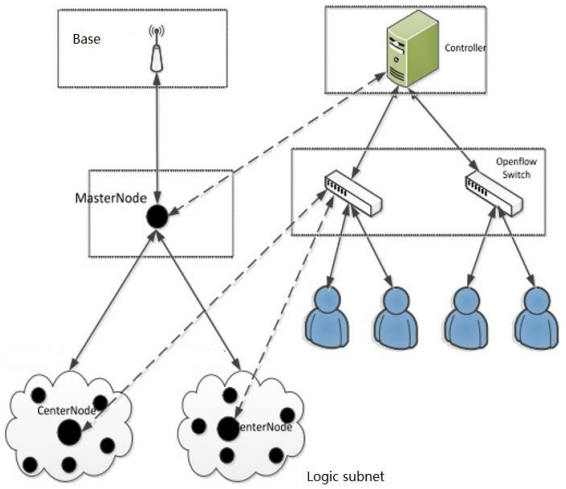

Figure 1. The intrusion detection structure SDSN

The black dots represent ordinary nodes and are only responsible for collecting data. The collected data will be sent to the Centernode node, which has sufficient energy supply and high computing power. The data sent to the Centernode node will be fused and processed at Centernode, and then sent to the Masternode node.

1. Masternode provides a user interface, so it has a strong programmability and scalability. The users can deploy customized detection rules and detection algorithms in real time according to the situation of the network. Masternode is responsible for logic control, data fusion and network security supervision in the whole WSN network. The Centernode deployed in the network feeds back the data information of each logical subnet to the Masternode which completes the aggregation and analysis of the information.

Masternode executes detection strategy at any time point according to the predefined detection algorithm:

1) The implementation of network traffic anomaly detection algorithm starts at Masternode node. The Hurst value calculated on the data in a time series. If the Hurst value of a time series is between 0.5 and 1, the network is not intruded. The Hurst value between 0-0.5 indicates an intrusion.

2) If the Hurst value is between 0 and 0.5, we need to determine which logical subnet is invading. At this point, the Master node, also known as the controller node, the network traffic anomaly detection strategy continues to compute the Hurst value of the data traffic sent from each subnet.

3) If the Hurst value of the network traffic of a logical subnet is not between 0.5-1, the data traffic of the subnet is abnormal. At this time, the cluster head node of the subnet generates a corresponding coping strategies to prevent the abnormal behavior of the network traffic.

The Centernode detection module is the second level abnormal response center of the network. The Centernode module responds only when Masternode detects that the subnet does not conform to self-similarity features. The Centernode module includes data collection module, data analysis module and exception response module. In the logical subnet, Centernode is the monitoring center of the whole subnet. It is responsible for receiving the data information which is sent by ordinary nodes in the subnet, and monitoring and analyzing the data information. Data analysis module is the core of Centernode.

Each node in the subnet sends the collected data information to the Centernode. Compared with OpenFlow switch, the time segment threshold for data forwarding can be set to a reasonable, small range due to the limited storage capacity of the Center Node. It is consistent with the time threshold of the Master Node, and must be consistent.

The Centernode node is responsible for the functions of OpenFlow switches. The stream table contains the packet header information of normal node sending data, such as packet size, sending frequency, packet type, forwarding port, destination address, source address and so on. At this point, the Centernode node matches the packet information sent by each ordinary node with the stream item information. If the match is successful, the node is normal. If the match is unsuccessful, it indicates that the node has

an exception. When an abnormal occurs, corresponding measures are taken to handle the abnormal nodes safely and effectively.

Centernode node will respond positively to network traffic anomalies caused by network intrusion. The response can be divided into two aspects: negative response and positive dynamic response. The negative response usually only reports the network status to the upper level. The typical network dynamics include sending alarm information, modifying network logs, and feeding back network intrusion behavior information to the upper layer. On the contrary, active and dynamic response, including the termination of the currently working data sending process, the immediate and effective blocking of the source of intrusion. It is a more effective response to intrusion. In order to reduce the loss of the network due to intrusion, Centernode can isolate the intruding nodes according to the actual network situation when the number of intruding nodes is small (such as 1-5). The Master node can redeploy network protocols if there are more intrusive nodes or attacked nodes too many to cause network instability.

2.2 The self-similarity of network

In the early 1990s, Leland et al. first proposed self-similarity which is exist in network traffic by analyzing LAN traffic. A series of traffic detection results on LAN and WAN indicate that network traffic shows strong self-similarity. A large number of scientific studies have shown that under normal network communication, the overall network traffic is usually self-similar [4].

When there is an attack in the network, a large number of connection requests or packet attacks will make the normal node unable to deal with. This situation leads to the energy exhaustion of normal nodes or blocking the transmission of normal packets. In this case, the self-similarity of the network will be affected. Therefore, we can use the parameters describing the self-similarity of the network to judge whether there is abnormal behavior at the node.

Self-similar formula: Let X={Xj,j=1,2,…} be a covariance stationary random sequence, that is, X has a constant value μ=E[X_j] and a finite variance$\sigma^2 = E[(X_j - \mu)]^2$. The autocorrelation function $r(k) = E[(X_j - \mu)(X_j + 1 - \mu)]/\sigma^2$ is only related to k, that is $r(k) = E[(X_j - \mu)(X_j + 1 - \mu)]/\sigma^2$, where 0<β<1. For $\forall x > 0$, L1 satisfies $\lim_{n\to\infty} \frac{L_1(tx)}{L_1(t)} = 1$. Let $Xk(m) = (Xkm - m + 1 + Xkm - m + \cdots + Xkm)/m$,k=1,2, 3… be the m-order aggregation process of X, set r(m),m=1,2,3,… is the autocorrelation function of time series $X(m) = (X1(m), X2(m), \ldots)$, H=1- β /2 is the autocorrelation parameter.

Self-similar features can be described by global scale Hurst values. The relationship between different scale converge can be obtained by the following simplified formula

$$x(t) = a - H_x \ (at)$$

From the above formula, it can be concluded that Hurst exponent H controls the network traffic curve relationship between different time series. If the Hurst exponent is between (0.5-1), it shows that the network traffic conforms to the self-similarity feature. With the increase of H value, the network self-similarity is stronger.

2.3 The process design of intrusion detection

In the logical subnet, the data collected by the collection node is sent to the Centernode node. Since the frequency of data collection and transmission is the same, that is to say, the amount of data sent to the Centernode node in unit time is the same. Normally, the amount of data sent to the Centernode node per unit time is the same, and the data traffic sent by the Centernode node to the Masternode node is also consistent, and there is no fluctuation in the amount of data

However, the storage capacity and computing capacity of nodes in wireless sensor networks are limited, and the calculation of large amounts of data will cause enormous energy consumption. When we find that there is an abnormality in the network, the communication of the network may last for a long time. It is obviously unrealistic to require the sensor to calculate such a large amount of data.

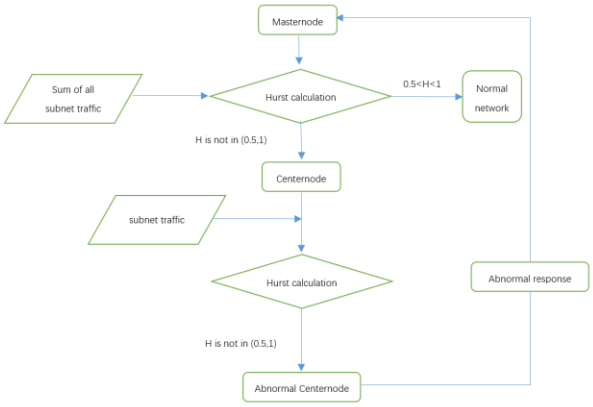

Figure 2. Iterative computation of Hurst Flow chart

At this point, the iterative calculation of Hurst value will solve the above problems. The specific strategy is as follows:

1. We can set a time threshold for Masternode nodes and Centernode nodes, such as 10 minutes. The Hurst is calculated every ten minutes. This results that the sensor node has very little storage. Because we don't need to save the network data in 10 minutes after calculating the Hurst value.

2. When the Hurst value of the network traffic is not consistent with the self-similar feature in the first 10 minutes, we need to calculate the Hurst value for the data traffic sent from each subnet. This is to determine which subnet's data traffic does not conform to the self-similar feature. In this way, it is very good to determine the subnet where traffic anomalies occur, that is to improve the accuracy of intrusion detection.

3 simulation test (ID simulation)

In a wireless sensor network, the frequency at each node

which collects data is consistent, and the rate of send data to the Centernode is consistent. If there is no node intruded, the data flow received by the Centernode node is consistent during the same time. This paper uses Mininet to create a wireless sensor network that supports SDN.

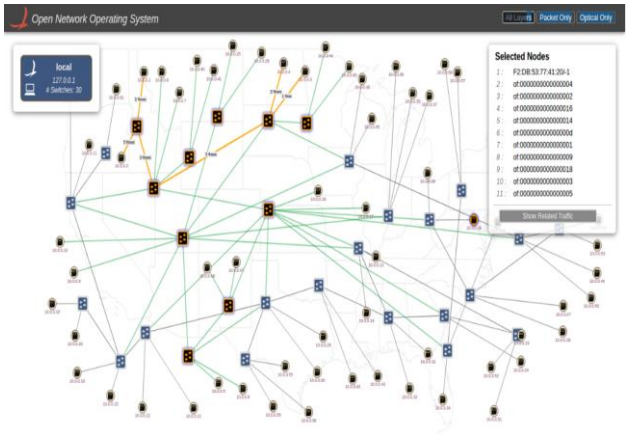

Figure 3. Experimental topology

The packets are captured with Wireshark deployed under Contiki. After processing the required data packets, the Hurst values are calculated by the obtained data. In this paper, R/S analysis is used to estimate the Hurst value to detect the self-similarity of traffic. The principle of R/S analysis is that the original time series is divided into data blocks of M size, and the mean and variance of each data block are calculated for each given M. Finally, the logs of M and sample variance are plotted as the horizontal and vertical axes respectively. Assuming that a node in the network is intruded, the data stream value of a common node is changed, and the contrast diagram of the self-similarity h value of the Centernode and the intrusion node is obtained as follows:

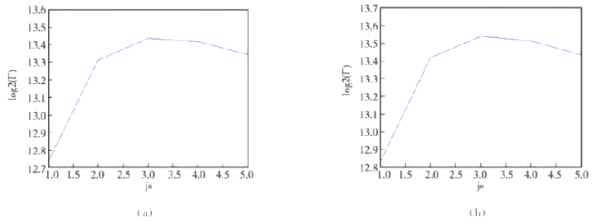

Figure 4. Self-similar characteristics under normal communication

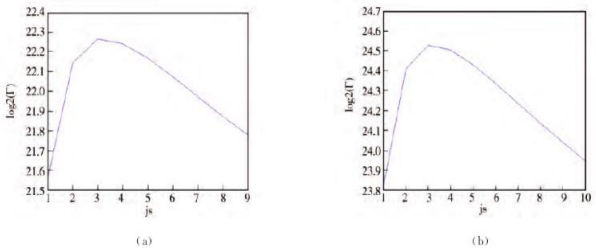

Figure 5. The self-similar characteristic when attacked

When a node or multiple nodes in the network intruded, the similarity coefficient value of the total network traffic changes dramatically. In the condition that the maximum value is significantly larger than the normal network, the similarity coefficient value drops sharply for a period of time after the maximum value appears. By calculating the Hurst value of network parameters with self-similar feature, it can be judged whether the network is intruded, which simplifies the complexity of intrusion detection.

4 Conclusion

With the OpenFlow technology, more WSN node energy consumption and network load balancing solutions can be provided. Through the analysis of various network attacks in a traditional network, an attacker first invades a node that is relatively easy to attack, and then latent until other attacking nodes to obtain higher privileges to start the attack. The Traditional intrusion detection schemes are easy to cause energy holes in the network because of unequal energy consumption of nodes. Therefore, detection around the key nodes can reduce the amount of data required for intrusion detection. At the same time, the detection efficiency can be improved and the node energy consumption of the whole network can be reduced.

Acknowledgements

This research is supported by the Program of Educational Commission of Anhui Province under Grants KJ2017A104, National Natural Science Foundation of China under Grants 61501005, which are gratefully acknowledged.

References

1. Sachin Sharma,Dimitri Staessens,Didier Colle,Mario Pickavet,Piet Demeester. OpenFlow: Meeting carrier-grade recovery requirements[J]. Computer Communications,2013,36(6).
2. Hui Yang,Jie Zhang,Yongli Zhao,Yuefeng Ji,Jianrui Han,Yi Lin,Shaofeng Qiu,Young Lee. Experimental demonstration of time-aware software defined networking for OpenFlow-based intra-datacenter optical interconnection networks[J]. Optical Fiber Technology,2014,20(3).
3. Yuanyu Wang,Hui Yang,Qilong Zhang. Phase structure and polar characteristics of alkali niobate ceramics modified by Ba 0.6 Ca 0.4 ZrO 3[J]. Ceramics International,2016,42(1).
4. Towards a secure controller platform for OpenFlow applications. Wen Xitao,Chen Yan,Hu Chengchen,Shi Chao. Proceedings of the ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN13). 2013
5. Etsuji Tomita,Akira Tanaka,Haruhisa Takahashi. The worst-case time complexity for generating all maximal cliques and computational experiments[J]. Theoretical Computer Science,2006,363(1).
6. Mohammad Al-Fares,Alexander Loukissas,Amin Vahdat. A scalable, commodity data center network architecture[J]. ACM SIGCOMM Computer Communication Review,2008,38(4).