International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 2 | Jan-Feb 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Optimized Intrusion Detection System using Deep Learning Algorithm

Prof P. Damodharan[1], K. Veena[2], Dr N. Suguna[3]

[1]Associate Professor, [2]PG Scholar, [3]Professor
Akshaya College of Engineering and Technology, Kinathukadavu, Coimbatotre, Tamil Nadu, India

ABSTRACT
A method and a system for the detection of an intrusion in a computer network compare the network traffic of the computer network at multiple different points in the network. In an uncompromised network the network traffic monitored at these two different points in the network should be identical. A network intrusion detection system is mostly place at strategic points in a network, so that it can monitor the traffic traveling to or from different devices on that network. The existing Software Defined Network (SDN) proposes the separation of forward and control planes by introducing a new independent plane called network controller. Machine learning is an artificial intelligence approach that focuses on acquiring knowledge from raw data and, based at least in part on the identified flow, selectively causing the packet, or a packet descriptor associated with the packet. The performance is evaluated using the network analysis metrics such as key generation delay, key sharing delay and the hash code generation time for both SDN and the proposed machine learning SDN.

1. INTRODUCTION

1.1. NETWORK SECURITY

A series of devices or computing nodes interconnected by communication link that allow to share and exchange the data among all devices is defined by the term 'Network'. A device can be anything which is capable of sending or receiving the data that is generated by the device and that is exchanged over the medium or channel. In other words, more than one autonomous computer is grouped together to exchange the information using the communication channel is called as 'Network'. In computer networks, the following characteristics or factors are mainly used to classify the various types of networks.

1.2. INTRUSION DETECTION SYSTEM

An Intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized entry or malicious activity. The ultimate aim of any IDS is to catch perpetrators in the act before they do real damage to resources. An IDS protects a system from attack, misuse, and compromise. It can also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. Intrusion detection system (IDS) is software that automates the intrusion detection process. The primary responsibility of IDS is to detect unwanted and malicious activities.

Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

1.3. NETWORK INTRUSION DETECTION

A Network intrusion detection system (NIDS) is a combination of hardware and software that monitors a computer network for attempts to violate a security policy. Network intrusion detection system identifies and eliminates misbehaving malicious in the network. A NIDS is a system that analyzes the traffic crossing the network, classifies packets according to header, content, or pattern matching, and further inspects payload information with respect to content/regular-expression matching rules for detecting the occurrence of anomalies or attacks. FPGA combined FA based NIDS efficiently handles the anomaly and intruded packet in the network.

Network intrusion detection systems (NIDS) are an important tool to protect network systems from external attack. NIDS are used to identify and analyze packets that may signify an impending threat to organization's network. Traditional software-based NIDS architectures are becoming strained as network data rates increase and attacks intensify in volume and complexity. In recent years, researchers have proposed using FPGAs to perform the computationally-intensive components of a NIDS.

MODEL BASED INTRUSION DETECTION

It states that certain scenarios are inferred by certain other observable activities. If these activities are monitored, it is possible to find intrusion attempts by looking at activities that infer a certain intrusion scenario. The model-based scheme consists of three important modules. The anticipator uses the active models and the scenario models to try to predict the next step in the scenario that is expected to occur. A scenario model is a knowledge base with specifications of intrusion scenarios. The planner then translates this hypothesis into a format that shows the behavior, as it would occur in the audit trail. It uses the predicted information to plan what to search for next. A NIDS aims at detecting possible intrusions such as a malicious activity, computer attack or computer misuse, spread of a virus, etc, and alerting the proper individuals upon detection.

2. LITERATURE SURVEY

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the two most harmful but easy to launch attacks: 1) spoofing attacks and 2) Sybil attacks. In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks.

For instance, in an IEEE 802.11 network, it is easy for an attacker to modify its Media Access Control address of Network interface card to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless Access point or an authorized client, an attacker can launch Denial-of-service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. On the other hand, in Sybil attacks, a Sybil node can forge different identities to trick the network with multiple fake nodes. The Sybil attack can significantly reduce the network performance by defeating group-based voting techniques and fault-tolerant schemes.

Therefore, identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks. It is thus desirable to detect the presence of identity-based attacks and eliminate them from the network. The traditional approach to address identity-based attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication.

Detecting the presence of identity-based attacks in the network provides first order information toward defending against attackers. Furthermore, learning the physical location of the attackers allows the network administrators to further exploit a wide range of defense strategies. This explore and how can find the positions of the adversaries by integrating our attack detector into a real-time indoor localization system. Our cluster-analysis-based attack detector is not specific to any RSS-based localization algorithms and is thus general. For two kinds of algorithms, area- and point-based algorithms, show that using the centroids of the clusters that are returned by the attack detector in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

Kerberos Authentication System

The Kerberos authentication system was introduced by MIT to meet the needs of Project Athena. It has since been adopted by a number of other organizations for their own purposes, and is being discussed as a possible standard. These problems fall into several categories. Some stem from the Project Athena environment. Kerberos was designed for that environment; if the basic assumptions differ, the authentication system may need to be changed as well. Other problems are simply deficiencies in the protocol design. Some of these are corrected in the proposed version 5 of Kerberos, but not all.

Kerberos is a security system. The functionality and efficiency, our primary emphasis is on the security of Kerberos in a general environment. This means that security-critical assumptions must be few in number and stated clearly. For the widest utility, the network must be considered as completely open. Specifically, the protocols should be secure even if the network is under the complete control of an adversary. This means that defeating the protocol should require the adversary to invert the encryption algorithm or to subvert a principal specifically assumed to be trustworthy. Only such a strong design goal can justify the expense of encryption.

Authorization Model And Access Control

In this section, discuss about the secure information sharing using the hierarchical path. Our focus is on maintaining the hierarchy rather than maintaining a shortest path. U sage policy: If user is authorized to access data of a particular level in the network, then it performs the operation as many times he wants. Essentially there is no predefined usage control. In this model, the authorization starts with the level selection of the network. At the time of choosing the levels, the nodes can have their keys for the secure communication. A node can have different paths to reach to other nodes; it can choose any particular path based on the preference.

Attribute-Based Access Control: This kind of access control uses attribute-based encryption techniques in which a sender encrypts a data packet with an access policy and a receiver decrypts the packet and reads its content only if its attributes satisfy the access policy. An example of the schemes which use such techniques is called Secure symptom based handshake (SSH).

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. In other words, it means that no one can gain, read, or manipulate information other than for whom it is intended. Basically, confidentiality is achieved in two steps: encryption and decryption. Using encryption, the sender converts plaintext to ciphertext with the aim of rendering it unintelligible to parties except the intended recipient. Using decryption, ciphertext is rendered intelligible to the intended recipient by converting it back to the plaintext.

3. EXISTING SYSTEM

Cross Layer Design

Cross layer design, where the boundary among the protocol layers is a violated by sharing internal information, helping layers to become aware of the changes in the others and provide higher quality of services to the user. To allow communication between layers by permitting one layer to access the data of the layer to exchange information and enable integration. Cross-layer designs involve cross-layer signaling which is not defined in the protocol architecture. These signaling methods should consume as scarce resources as possible reducing the overhead.

Packet headers: Information can be encoded in layer headers which can later be used by some other layer to glean the desired information. This can be compared to have pipe like flow of signals among the layers.

ICMP messages: In IP based networks, Internet Control Message Protocol (ICMP) messages can be used for signaling. However, as ICMP messages are always encapsulated by IP packets, the messages have to traverse through the network layer, even if the interacting layer pairs are data link and physical or transport and application.

The estimation of link available bandwidth from mac layer information that take into account the activities of the node's neighbours and adapt to change of channel condition dynamically is used in the network layer to provide efficient routing. And radio selection and channel assignment from physical layer is used, Best-effort traffic and Real-time traffic from application layer is used to provide QoS guarantee for real-time multimedia applications.

Network layer:
It is main layer which executes the DAWN process. The following procedures are implemented in network layer itself.

1. Traffic classification
2. Executing physical routing
3. Logical routing from bandwidth information

Mac layer:
Like all 802.11 network, nodes broadcasts RTS, CTS, Data acknowledge handshake process and complete the transmission for all packet. And each time of transmission node maintains the used bandwidth value and calculates remaining raw bandwidth value. Then idle duration is calculated for each node. And available bandwidth value is calculated from raw and idle values.

Physical layer:
Channel assignment and interface switching process is executed in this layer. By selecting the maximum CSI value interface to be selected for transmission is identified.
Security Management

SSL Certificates have a key pair: a public and a private key. Device connects to a web server (website) secured with SSL (https). Device requests that the server identify itself. Server sends a copy of its SSL Certificate, including the server public key. Device checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the Device trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the servers public key. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

The cryptographic parameters of the session state are produced by the SSL handshake protocol, which operates on top of the SSL record layer the client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail. The client hello and server hello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method.

Following the hello messages, the server will send its certificate, if it is to be authenticated. Additionally, a server key exchange message may be sent, if it is required .If the server is authenticated, it may request a certificate from the client, if that is appropriate to the cipher suite selected. Now the server will send the server hello done message, indicating that the hello-message phase of the handshake is complete. The server will then wait for a client response. If the server has sent a certificate request message, the client must send either the certificate message or a no certificate alert. The client key exchange message is now sent, and the content of that message will depend on the public key algorithm selected between the client hello and the server hello. If the client has sent a certificate with signing ability, a digitally-signed certificate verify message is sent to explicitly verify the certificate.

At this point, a change cipher spec message is sent by the client, and the client copies the pending CipherSpec into the current CipherSpec. The client then immediately sends the finished message under the new algorithms, keys, and secrets. In response, the server will send its own change cipher spec message, transfer the pending to the current CipherSpec, and send its finished message under the new CipherSpec. At this point, the handshake is complete and the client and server may begin to exchange application layer data.

```
Client                                    Server

Client Hello                    -------->
Server Hello

Certificate*
Server Key Exchange*
Certificate Request*
<--------    ServerHelloDone
    Certificate*

Client Key Exchange
Certificate Verify*
    [Change Cipher Spec]
    Finished                -------->

[ChangeCipherSpec]
<--------               Finished
    Application Data     <------->     Application Data
```

*Indicates optional or situation-dependent messages that are notalways sent.

4. IMPLEMENTATION

Implementing and using SSL to secure HTTP traffic
Security of the data stored on a file server is very important these days. Compromised data can cost thousands of dollars to company. In the last section, compiled LDAP authentication module into the Apache build to provide a Authentication mechanism. However, HTTP traffic is very insecure, and all data is transferred in clear text - meaning, the LDAP authentication (userid/passwd) will be transmitted as clear text as well. This creates a problem. Anyone can sniff these userid/passwd and gain access to DAV store. To prevent this encrypt the HTTP traffic is essentially as HTTP + SSL or HTTPS. Anything transferred over HTTPS is encrypted, so the LDAP userid/passwdcan not be easily deciphered. HTTPS runs on port 443.

Introduction to SSL
SSL is a protocol layer that exists between the Network Layer and Application layer. As the name suggest SSL provides a mechanism for encrypting all kinds of traffic - LDAP, POP, IMAP and most importantly HTTP.

Encryption algorithms used in SSL

There are three kinds of cryptographic techniques used in SSL: Public-Private Key, Symmetric Key, and Digital Signature.

Public-Private Key Crytography - Initiating SSL connection: In this algorithm, encryption and decryption is performed using a pair of private and public keys. The Web-server holds the private Key, and sends the Public key to the client in the Certificate.

The following is a over-simplified structure of the layers involved in SSL.

```
+-------------------------------------------+
      | LDAP | HTTP | POP | IMAP |
+-------------------------------------------+
               |  SSL  |
+-------------------------------------------+
            | Network Layer |
+-------------------------------------------+
```

1. The client request content from the Web Server using HTTPS.
2. The web server responds with a Digital Certificate which includes the server's public key.
3. The client checks to see if the certificate has expired.
4. Then the client checks if the Certificate Authority that signed the certificate, is a trusted authority listed in the Device. The client then checks to see if the Fully Qualified Domain Name (FQDN) of the web server matches the Comman Name (CN) on the certificate?

Anything encrypted with Private Key can only be decrypted by using the Public Key. Similarly anything encrypted using the Public Key can only be decrypted using the Private Key. There is a common mis-conception that only the Public Key is used for encryption and Private Key is used for decryption. This is not case. Any key can be used for encryption/decryption. However if one key is used for encryption then the other key must be used for decryption. e.g. A message cannot encrypted and then decrypted using only the Public Key.

Using Private Key to encrypt and a Public Key to decrypt ensures the integrity of the sender (owner of the Private Key) to the recipients. Using Public Key to encrypt and a Private Key to decrypt ensures that only the inteded recipient (owner of the Private Key) will have access to the data.(i.e. only the person who holds the Private Key will be able to decipher the message).

Symmetric Cryptography - Actual transmission of data: After the SSL connection has been established, Symmetric cryptography is used for encrypting data as it uses less CPU cycles. In symmetric cryptography the data can be encrypted and decrypted using the same key. The Key for symmetric cryptography is exchanged during the initiation process, using Public Key Cryptography.

Message Digest The server uses message digest algoritm such as HMAC, SHA-1, MD5 to verify the integrity of the transferred data.

Ensuring Authenticity and Integrity
Encryption

Step1: In this step the Original "Clear Text" message is encrypted using the Sender's Private Key, which results in Cipher Text 1. This ensures the Authenticity of the sender.

Step2: In this step the "CipherText 1" is encrypted using Receiver's Public Key resulting in "CipherText 2". This will ensure the Authenticity of the Receiver i.e. only the Receiver can decipher the Messsage using his Private Key.

Step3: Here the SHA1 Message Digest of the "Clear Text" is created.

Step4: SHA1 Message Digest is then encrypted using Sender's Private Key resulting in the Digital Signature of the "ClearText". This Digital Signature can be used by the receiver to ensure the Integrity of the message and authenticity of the Sender.

Step5: The "Digital Signature" and the "CipherText 2" are then send to the Receiver.

SSL Certificates have a key pair: a public and a private key.

1. Device connects to a web server (website) secured with SSL (https). Device requests that the server identify itself.
2. Server sends a copy of its SSL Certificate, including the server's public key.
3. Device checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the Device trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. Server decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. Server and Device now encrypt all transmitted data with the session key.

The cryptographic parameters of the session state are produced by the SSL handshake protocol, which operates on top of the SSL record layer. When an SSL client and server first start communicating, they agree on a protocol version, select cryptographic algorithms, optionally authenticate each other, and use public key encryption techniques to generate shared secrets. These processes are performed in the handshake protocol, which can be summarized as follows: the client sends a client hello message to which the server must respond with a server hello message, or else a fatal error will occur and the connection will fail.

A cryptography system design which are related to generation, exchange, storage, safeguarding, use, vetting, and replacement of keys in key management. It includes cryptographic protocol design which includes key servers, user procedures, and other relevant protocols. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Successful key management is critical to the security of a cryptosystem.

SCALABILITY

The ability of a system, network, or process, to handle growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth. Scalability, as a property of systems, is generally difficult to define and in any particular case it is necessary to define the specific requirements for scalability on those dimensions that are deemed important. It is a highly significant issue in electronics systems, databases, routers, and networking. A system whose performance improves after adding hardware, proportionally to the capacity added, is said to be a scalable system. An algorithm, design, networking protocol, program, or other system is said to scale,(e.g. a large input data set or a large number of participating nodes in the case of a distributed system). If the design fails when the quantity increases, it does not scale.

focuses on well-understood security attributes and features such as integrity, authentication, authorization, key management, and intrusion detection. A classification of IDS risks and vulnerabilities has recently been published by NIST. Working mechanism is as follows:Initially network is deployed with server, router, commander and DDOS attackers

1. Communication tree is formed between all wireless devices using the router nodes as interface
2. Commander node initiates the DDOS attack by sending the command message with victim id to all DDOS attackers present in the network.
3. Command message is rebroadcasted to all DDOS attackers and it launches the attack to reduce the availability of resource of the victim node.
4. Flow monitoring is performed by all router nodes which validate the each incoming flows.
5. It computes the data generation rate of each monitoring flow and performs the IP trace back

IDS algorithm

1. Once the network deployment gets completed, data transmission is originated between source and destination.
2. A network device may fail to forward a packet due to various reasons.
3. During the situation, the devices generates the ICMP error message (path backscatter message)
4. But the packet contains the IP spoofed id as source id, then the packet will sent to the source IP address indicated in the original packet ie., the node who owns the actual ip address
5. The ICMP message is generated during the high class congestion occurred in the data transmission

The proposed system is designed by using the principle component analysis. The proposed approach working mechanism is as follows:

1. Network is deployed with set of mobile nodes including major and minor player
2. Data transmission is initiated between mobilenodes by forming the multihop route
3. DOS attacker nodes launches attacks against victim node (src and dst nodes)
4. Packet is captured and either dropped or content is changed by the DOS attacker
5. Major and minor player game is invoked between mobile nodes to perform the detection process
6. IDS nodes performs the data validation and attack detection process by applying the Machine Learning.

The proposed system is designed by using the reinforcement learning in the machine learning model which significantly improves accuracy of the intrusion and anomaly detection system by employing the learning process using the Boltzmann learning parameters. During the data transmission, packet drop process and packet delaying can be occurred due to the congestion and the collision along with the unavailability of the channel beau case of the hidden terminal and exposed terminal problem. This will lead to the false detection of the normal behaviour as malicious behaviour in the network environment. In order to handle this network dynamics, the learning system is employed based on the reinforcement learning system.

1. The behavioural prediction and decision making system is operated from the input collected during the learning process.
2. From the collected input, the collaborated view of the hidden layer is formed by using the dynamic Bayesian network with Boltzmann input.
3. The Dynamic Bayesian Network is constructed with the 3 input models,
   A. Inference model
   B. Parameter learning
   C. Structured learning
4. The inference system collects the variation between the Actual state and the expected state after performing the initial IDS
5. For each inferences identified in the system, the collected parameters are differentiated with respect to the identified behaviour of the node and channel in terms of state information in the parameter learning process.

A deep Boltzmann machine (DBM) is a recently introduced Markov random field model that has multiple layers of hidden units. It has been shown empirically that it is difficult to train a DBM with approximate maximum-likelihood learning using the stochastic gradient unlike its simpler special case, restricted Boltzmann machines (RBM)Deep Boltzmann machine (DBM) is a recently introduced variant of Boltzmann machines which extends widely used restricted Boltzmann machines (RBM) to a model that has multiple hidden layers. It differs from the popular deep belief network (DBN) which is built by stacking multiple layers of RBMs. DBMs facilitate propagating uncertainties across multiple layers of hidden variables. Although it is straightforward to derive a learning algorithm.

Deep Boltzmann machines are interesting for several reasons. First, like deep belief networks, DBM's have the potential of learning internal representations that become increasingly complex, which is considered to be a promising way of solving object and speech recognition problems. Second, high-level representations can be built from a large supply of unlabeled sensory inputs and very limited labeled data can then be used to only slightly fine-tune the model for a specific task at hand. Finally, unlike deep belief networks, the approximate inference procedure, in addition to an initial bottom up pass, can incorporate top-down feedback, allowing deep Boltzmann machines to better propagate uncertainty about, and hence deal more robustly with, ambiguous input.

RESULT AND DISCUSSION

OPERATIONAL ENVIRONMENT

The real world testing process is done in C#.net environment by running the working design using the validation metrics. This analysis is used to test the performance of the existing protocols as well as newly derived protocols.The performance evaluation is conducted to validate the execution of the proposed technique in terms of packet related metrics such as key generation and key sharing delay, hash code generation delay. The table shows that the parameters used to perform the network performance validation.

Key Sharing Delay: Sharing Delay refers the Time taken to complete the key sharing process from user device to server in the network using equation (2).

$$\begin{aligned}&\mathit{Key\ SharingDelay} = \\ &\mathit{Key\ Sharing\ Completed\ Time} - \\ &\mathit{Key\ Generation\ Initiated\ Time}\end{aligned} \tag{2}$$

Hash Generation Delay: Hashing delay refers the time required to complete the hash code generation and it is estimated using equation (3).

$$\begin{aligned}&\mathit{HashingDelay} = \\ &\mathit{HashCode\ Generation\ Completed\ Time} - \\ &\mathit{Hash\ Code\ Generation\ Initiated\ Time}\end{aligned} \tag{3}$$

5. PERFORMANCE EVALUATION

Figure 1, 2 and 3 shows the comparisons between Software Defined Network (SDN) and Machine Learning Software Defined Network (MLSDN) in terms of Key Generation Delay, Key Sharing Delayand Hash Generation Delay respectively. It outcomes in key generation process and key sharing process. In case of Key Generation Delay, MLSDN achieves higher performance by obtaining the lower delay. Similarly for Key SharingDelay MLSDN in lower latency compare to SDN. In case of Hash Generation Delay, MLSDN achieves lower delay while generating the hash code.

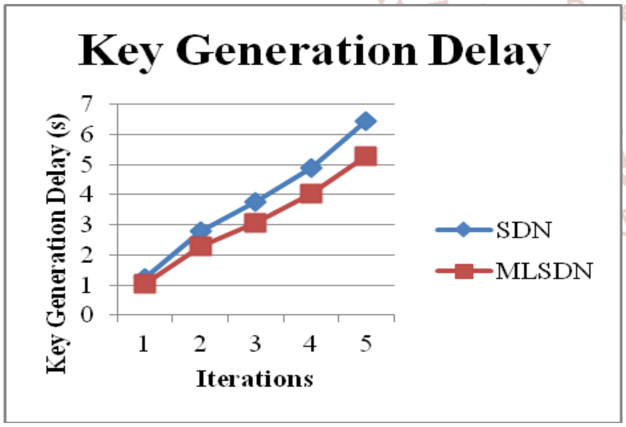

Figure7.1. Key Generation Delay

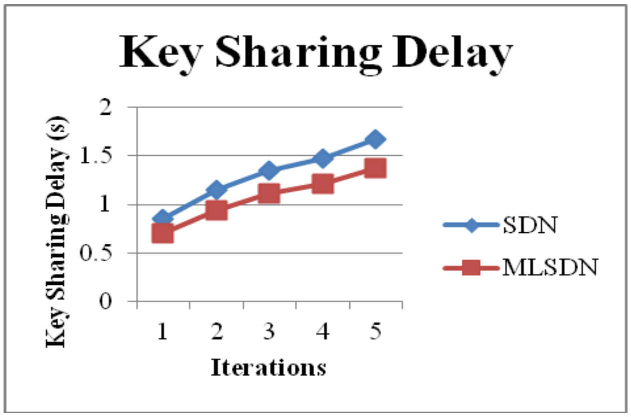

Figure7.2. Key Sharing Delay

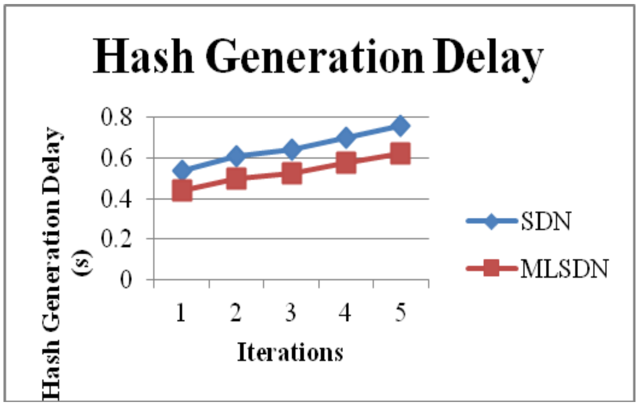

Figure7.3.Hash Generation Delay

Figure 4, 5 and 6 shows the average performance comparisons between SDN and MLSDN in terms of Key Generation Delay, Key Sharing Delayand Hash Generation Delay respectively.

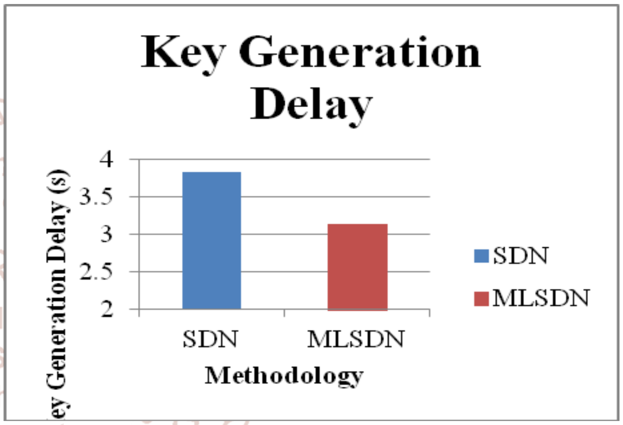

Figure7.4.Average Key Generation Delay

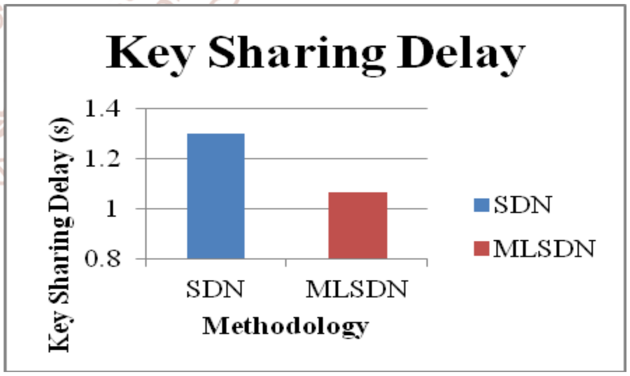

Figure7.5. Average Key Sharing Delay

CONCLUSION

The SDN model is the novel networking model which utilizes the separation of forward and control planes by introducing a new independent plane called network controller. The architecture enhances the network resilient, decompose management complexity, and support more straight forward network policies enforcement. Proposed IDS system analyzes the network activity for unauthorized entry or malicious activity using the machine learning algorithm instead of software defined network. Proposed system that analyzes the traffic crossing the network, classifies packets according to header, content, or pattern matching, and further inspects payload information with respect to content/regular-expression matching rules for detecting the occurrence of anomalies or attacks

FUTURE WORK

It can enhance by deep learning optimization scheme for secure channel processing. Compliance with real-time constraints: In real-time applications, data is delay constrained and has a certain bandwidth requirement. For instance, scheduling messages with deadlines is an important issue in order to take appropriate actions in real time. However, due to the interference and contention on the wireless medium, this is a challenging task. Multi-channel communication can help to reduce the delay by increasing the number of parallel transmissions and help the network to achieve real-time guarantees. Assignment of overlapping channels during run-time: Use of overlapping channels at run time during medium access is an interesting and challenging future research direction.

REFERENCES

[1] Khoshkbarforoushha, R. Ranjan, R.Gaire, E. Abbasnejad, L. Wang, and A. Y. Zomaya. Distribution based workload modelling of continuous queries in clouds. IEEE Transactions on Emerging Topics in Computing,5(1):120–133, 2017

[2] Benaloh.J, “Key Compression and Its Application to Digital Fingerprinting” technical report, Microsoft Research, 2009.

[3] D. D´ıaz-Pernil, A. Berciano, F. Pe˜na-Cantillana, and M. A. Guti´errez- Naranjo. Bio-inspired parallel computing of representative geometrical objects of holes of binary 2d-images. International Journal of Bio-Inspired Computation, 9(2):77–92, 2017.

[4] Chen, F., Ji, R., Su, J., Cao, D. and Gao, Y., 2018. Predicting Microblog Sentiments via Weakly Supervised Multimodal Deep Learning. IEEE Transactions on Multimedia, 20(4), pp.997-1007.

[5] Jiang, F., Fu, Y., Gupta, B.B., Lou, F., Rho, S., Meng, F. and Tian, Z., 2018. Deep Learning based Multi-channel intelligent attack detection for Data Security. IEEE Transactions on Sustainable Computing.

[6] G.-G. Wang, X. Cai, Z. Cui, G. Min, and J. Chen. High performance computing for cyber physical social systems by using evolutionary multi-objective optimization algorithm. IEEE Transactions on Emerging Topics in Computing, 2017. [26] L. Wang, H. Geng, P. Liu, K. Lu, J. Kolodziej, R. Ranjan,

[7] Lei, L., You, L., Dai, G., Vu, T.X., Yuan, D. and Chatzinotas, S., 2017, August. A deep learning approach for optimizing content delivering in cache-enabled HetNet. In Wireless Communication Systems (ISWCS), 2017 International Symposium on (pp. 449-453). IEEE.

[8] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y. and Gan, D., 2018. Cloud-based cyber-physical intrusion detection for vehicles using Deep Learning. IEEE Access, 6, pp.3491-3508.

[9] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar. A survey on malware detection using data mining techniques. ACM Computing Surveys(CSUR), 50(3):41, 2017

[10] Z. Cui, B. Sun, G. Wang, Y. Xue, and J. Chen. A novel oriented cuckoo search algorithm to improve dv-hop performance for cyber–physical systems. Journal of Parallel and Distributed Computing, 103:42–52, 2017.