IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 13, Issue 5 Ver. II (Sep-Oct. 2018), PP 57-63
www.iosrjournals.org

Enhancement of the Strategy Development Based Security Application in Social Defined Network Using Hill Cipher Algorithm

Mohini Prasad Mishra[1] Aurobinda Kar[2]
1(Department of Computer Science & Engineering, Gandhi Engineering College ,India)
2(Department of Computer Science & Engineering, Gandhi Institute For Technology, College)

Abstract: *The aim of this study is to develop a strategy based security applications to improve the software security defined network using modern proficient algorithm. It has a control model by the separation of the control plane and data plane. It's well suited to secure the network deployments and provides logically centralized intelligence programmability. But, the software defined network suffers from denial of service attacks in most cases. To overcome this crisis, security algorithm has been proposed to protect the network and investigated the security assets on the software defined network control channel and required algorithm to overcome the security problem. Hill cipher algorithm is used for providing authentication to secure the software defined network. This analysis is focused on performance of various routing protocols running over software defined network by using the authentication mechanism. Performance metrics like throughput, end-to-end delay and packet delivery ratio were considered for analysis. The result shows that the destination sequenced distance vector routing protocol have better performance in software defined network.*
Key Word*: SDN, Security, DoS, Routing Protocol, DSDV Routing*

I. Introduction

In current scenario the new technique of Software Defined Network (SDN) manages network services through low-level functionality. SDN has a centralized controller that defines the behavior of the network. It enables the administrator to use simpler and more flexible network control and management. The controller manages the underlying network devices through an open and standardized Application Programming Interface (API). The control plane exchanges the information to data plane through the southbound application programming interface [1-4]. The centralized controller of the SDN had the global view of the entire network state, and can adapt to complex networks by reacting to network states and events. Each device in the network communicates with each other to coordinate network path construction. In a centralized control plane paradigm, a single-control plane would exist. This plane helps to push commands to manipulate its physical switching and routing for each device [5-8]. On comparing the software defined networks and traditional networks, SDN has centralized controller, where the other has distributed controller, shown in Figure 1. The way, the traditional network handles an incoming packet is written into its firmware and moreover, they are static and inflexible networks. According to SDN architecture, SDN is suitable for several networks such as data center, transport networks and mobile networks [9-12]. The SDN has the capacity to block certain packets by automatically prioritizing and ability to control switches that handles data. It enables to increase the efficiency without the need of application-specific network switches. The architecture of the SDN is categorized into three layers such as application layer, control layer and data layer as shown in Figure 2. The data plane composed of forwarding devices that performs a set of elementary operations. Each device forwards the incoming packets through a well-defined instruction sets [13-16]. The most important layer of the SDN is the control layer which keeps on tracking the topology and has the control of all the network devices in the infrastructure. The control layer exchanges the information of the network state with the application layer through the northbound API. The application layer consists of an application that works under the commands offered by the northbound interface with the network application includes load balancing, monitoring, firewalls, routing, etc. The research work focuses on improving network security in SDN. It monitors the system dynamically to detect suspicious traffic during real-time network operations [17-21]. One of the most common types of security problems in SDN is denial-of-service (DoS) attacks. The DoS attack makes the user's service unavailable, hence the sender be unable to provide the expected service to its customers. The goal of this paper is to design an authentication mechanism to prevent the SDN control channel from attacks. The proposed mechanism can be easily adopted by existing SDN switches [22-27]. The research work makes the contributions such as the possibility of DoS attack in the SDN controller, propose an authentication mechanism to protect SDN controller from DoS attacks and to perform simulation and make analyzes.

Strategy Development Based Security Application to Boost the Software Security Defined Network Using Modern Proficient Hill Cipher Algorithm

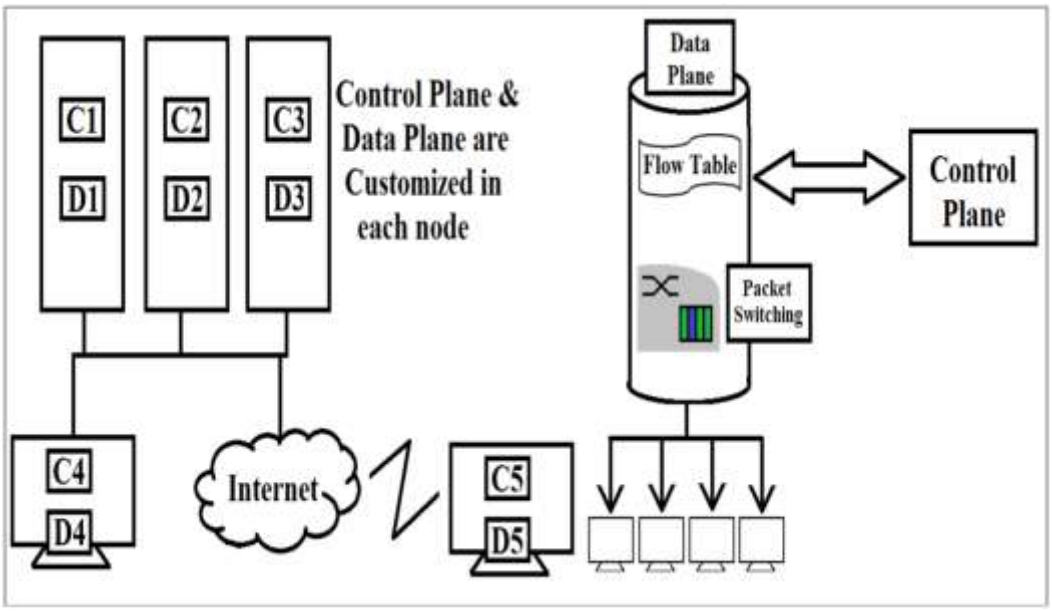

Figure 1 Traditional Network Vs Software Defined Network

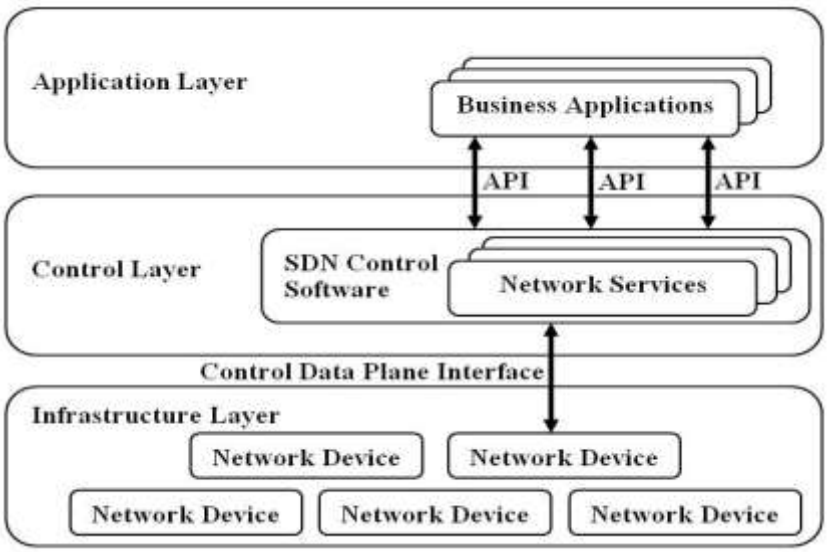

Figure 2 Structural Design of Software Defined Network

II. Analysis of performance and Security

2.1 Security for Control Channel

Security is the major concern when designing network architecture. SDN work focuses on enhancing the security and management of the networks. SDN improves the network security by providing the global view of the network. Separation of control plane and data plane puts the security efforts on controller. SDN security must be incorporated into the architecture to guarantee the availability of all connected devices. An open flow switch has more number of flow tables. Each flow table contains the flow entries and communicates with the controller. The SDN has the capability of managing multiple switches simultaneously. At the same time it suffers from conventional complexities such as dropping packets, delaying of the control packets. The stateful SDN data planes provide attention on the security implications by continuously monitoring the packets. The goal of the data plane is to overcome the limitations.

and to provide stateful operations inside the switches. The possible attack in SDN is denial of service, which can easily abuse the network. The DoS is an action that impairs the authorized use of systems, networks by exhausting resources. The two types of DoS attacks are insider and outsider DoS. The insider DoS attack is

an authenticated device within a legitimate network that communicate with other members in the network. The outsider DoS attack is an intruder considered by the network authenticated devices.

2.2 Security Assets

Networks that are built according to SDN architecture principles need to protect a number of key security assets like integrity which maintains trustworthiness and accuracy of the data, authentication is nothing but only authenticated users can access the SDN components. The authentication is used to identify hijacking and to limit the consequences of stolen credentials. Resiliency is the network should have the ability to recover as autonomously as possible from an attack and availability is the network should remain operational even under the cause of an attack. Finally, performance is the network should have the ability to guarantee a baseline bandwidth and latency even in the occurrence of an attack

III. Proposed Methodology

The security challenge is the combination of SDN and network vulnerabilities. The necessity to develop a secured SDN is to overcome the security issues by providing secured network architecture. The SDN controller will secure the data within each layer utilizing the packets for secured routing. The goal of the research is to ensure the network being protected from intruder. The proposed methodology focuses on one of the assets such as authentication, which secures communication between nodes through the mechanism used. Thus we compare traditional network with SDN to analysis the security performance. SDN provides the ability to easily program the network and can create dynamic flow policies. In the SDN architecture, a particular node is made to act as SDN controller that monitors the entire network, as all the switches are connected to that particular node. The process of the SDN controller is to encrypt the message and the decryption is made by the remaining nodes. The same architecture is compared for different routing protocols like Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) and Adhoc On-demand Distance Vector (AODV) with and without applying the authentication mechanism.

3.1 Certification Mechanism

The information hiding includes watermarking for copyright protection, steganography for secret communication and certification for genuine user verification. Unlike cryptography which provides secrecy through data scrambling, information hiding provides secrecy through obscurity. Security based network algorithm generally utilizes protocol or packet headers mechanism to hide information.

3.2 Hill Cipher Algorithm

The hill cipher algorithm is used for covered transmission of data. Each letter in the alphabets is represented by a number. Often the scheme, A=1, B=2....Z=26 is used. The encryption process is applied for SDN controller and decryption process is applied for the remaining nodes, to protect the messages. The key size for the algorithm is fixed to be 3x3matrix according to our process. To encipher this, the plaintext is break into chunks of 3 and performs matrix multiplication with the secret key mod26. The secret key is preferred only to the authenticated users to secure the secret information. The mentioned step is performed for every 3 letter blocks in the plaintext. After the completion of encryption, the ciphered text is passed to all the nodes. To decipher this, the encrypted message with 3 letter blocks is matrix multiplied with the inverse of the 3x3keysize mod26, to achieve the original text. This process helps to protect the secret message from intruders, until they know the key size.

Plaintext to Cipher text: $C = K \times P \pmod{26}$
Cipher text to Plaintext: $P = K\text{-}1 \times C \pmod{26}$
Where, K- Key size of the matrix 3x3

3.3 Routing Protocol

Routing protocols are to determine the specification of each link. The routing algorithm has a prior knowledge of the network state. Once the packets are sent, the routing protocols shares this information among the intermediate neighbors. This way, each node gains knowledge of the network. The routing protocols used for the SDN network are dynamic source routing, destination-sequenced distance vector, ad hoc on-demand distance vector.

IV. Result Discussion

With the simulation tool Network Simulator (NS)-2, the SDN concept is considered. The topology is connected with certain switches to check the state of each link. The hill cipher algorithm has been applied to the SDN network in order to overcome the intruder nodes. The Table 1 shown represents the parameter for NS-2

simulation. The parameters listed are supportable for SDN environment. As mentioned above, the three routing protocols are used to analysis the performance metrics and the results are manipulated for different values. SDN architecture is represented in the Figure 3 by separating control plane and data plane. The SDN controller communicates to its forwarding devices through an open flow switch. The switch maintains the flow entries of each node and communicates with the controller.

Table 1 Simulation Parameters

Parameters	Range
Channel Type	Wireless
Propagation model	Two-ray ground model
Mac type	Mac/802.11
Antenna model	Omni-Antenna
Network size	1000 x 700
Routing protocols	AODV, DSR, DSDV
Number of nodes	19
Simulation time	10 seconds

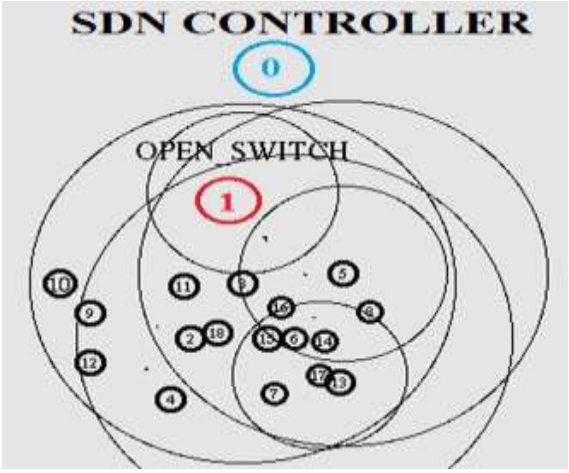

Figure 3 Architecture of SDN in Network Simulator 2

The traditional network is shown in Figure 4 which has distributed controllers working under the server. The server broadcast the message to the connected controllers. The controllers transmit the packets to its corresponding nodes.

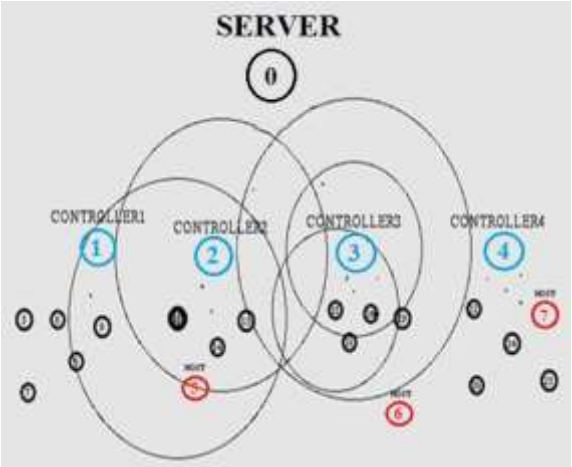

Figure 4 Traditional Network

In Figure 5, packet drop is seen at times, when more number of nodes send request to SDN controller at the same time. The packets are transmitted in a secret way and only the authenticated users are permitted to use the message. The SDN controller sends the encrypted message to all connected nodes. Then through the switch, the messages are sent to nodes. The decryption algorithm applied on the nodes convert the encrypted message into original message. So there will be proper transmission of messages without any attacks.

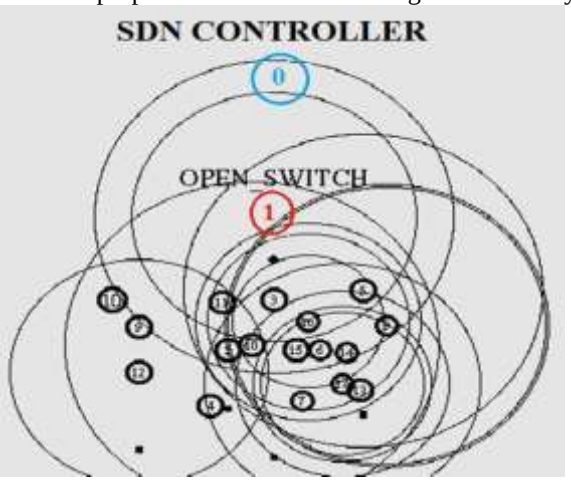

Figure 5 SDN Network Packet Drop

The Figure 6 represents throughput versus packet sent in SDN topology. The parameters are calculated after applying this algorithm for each node. The same procedure is repeated by increasing the number of packets. Finally all the obtained values are plotted for the three protocols. The throughput in network with SDN for DSDV protocol is higher than the other two routing protocols according to the graph. Figure 7 shows graph against end-to-end delay and packet sent in SDN topology. This end-to-end delay parameter has been determined for three protocols and it is observed to be less for DSDV protocol than the other two routing protocols according to the graph obtained. Similarly, Figure 8 shows comparison of three protocols for packet delivery ratio vs packet sent. Comparatively the packet delivery ratio for DSDV protocol is observed to be high in SDN network state than the other two routing protocols.

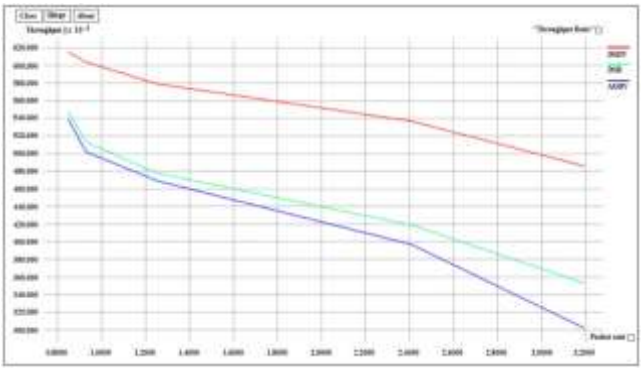

Figure 6 Packet Sent Vs Throughput

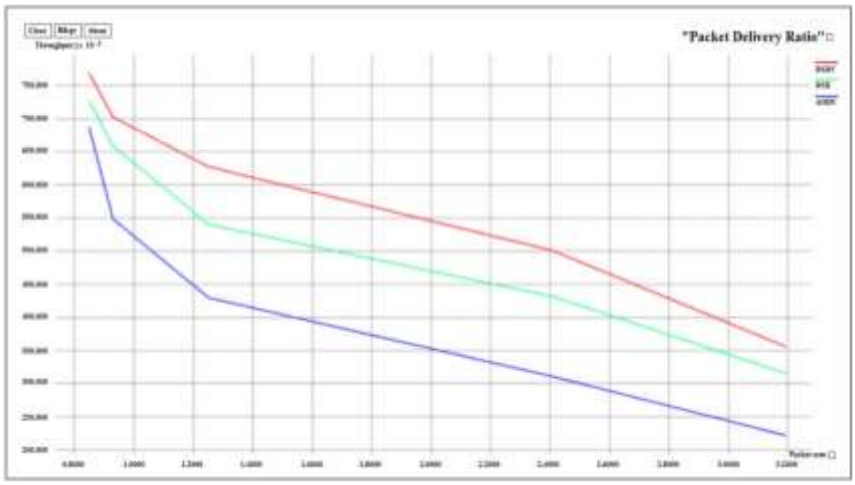

Figure 8 Packet Sent Vs Packet Delivery Ratio

The Table 2 shows the performance results calculated for the 3 routing protocols of DSDV, DSR and AODV. These metrics are calculated from trace file, obtained for each time while increasing the packets. Here the results are taken for 'n' packets sent and calculated for all 3 protocols and the differentiation is shown. The DSDV protocol is preferred for SDN, as it has greater efficiency than others.

Table 2 Results of DSDV, DSR and AODV

Parameters	DSDV	DSR	AODV
Packets sent	845	845	845
Packets received	650	610	580
Packets dropped	195	230	260
Total bytes	347610	315350	310120
Throughput (kbps)	602	548	540
Packet delivery ratio	0.77	0.73	0.69
End-to-end delay	0.24	0.30	0.35

V. Conclusion

The objective of policy development based security application to improve the software security defined network using modern proficient hill cipher algorithm was carried out. The SDN concept is considered especially from the perspective of network security and the security improvements are explored. From the results following conclusions were arrived.

•The possible threats towards SDN controller and other communication devices in SDN domain have been overcome by developing a policy based security application.

•This application is more protective to secure the SDN domain. Solutions are proposed for an enhanced security but still more research needs to be done to obtain highly secured network.

•Authentication mechanism is provided which secures the communication between nodes, thereby providing security.

•Different scenarios are created with SDN controller and performance metrics like throughput vs packet sent, end-to-end delay vs packet sent, packet delivery ratio vs packet sent are shown in graph.

•DSDV routing protocol provides higher packet delivery ratio, lesser delay and higher throughput for SDN as compared with other two protocols.

References

[1]. Alsmadi and Xu, D. Security of software defined networks- A survey. Computers and Security, 53, 2015, pp. 79-108.
[2]. N. Feamster, J. Rexford and E. Zegura. The road to SDN: An intellectual history of programmable networks. ACM Computer Communication Review, 44(2), 2014, pp. 87-98.
[3]. D. Sobya, SK. Muruganandham, S. Nallusamy and P.S. Chakraborty. Establishment of smart meter reading scheme for monitoring the power in residence using bluetooth. International Journal of Electrical Engineering and Technology, 9(1), 2018, pp. 67-75.
[4]. D. Sobya, S.K. Muruganandham, S. Nallusamy and Partha Sarathi Chakraborty. Bit error and data transmission rate augmentation through MIMO diversity technique. International Journal of Advanced Research in Engineering and Technology, 9(2), pp. 94-103.

[5]. S. Nallusamy. Overall performance improvement of a small scale venture using critical key performance indicators. International Journal of Engineering Research in Africa, 27, 2016, pp. 158-166.
[6]. Ahmad, S. Namal, M. Ylianttila and A. Gurtov. Security in software defined networks- A survey. Communications Surveys and Tutorials IEEE, 17(4), 2015, pp. 2317-2346.
[7]. D. Sobya, S. Nallusamy and Partha Sarathi Chakraborty. A proposed remote monitoring system by global system for mobile communication and internet technology. International Journal on Recent Researches in Science Engineering and Technology, 5(11), 2017, pp. 07-14.
[8]. S. Nallusamy, Sri Lakshmana Kumar, K. Balakannan and P.S.Chakraborty. MCDM tools application for selection of suppliers in manufacturing industries using AHP, Fuzzy Logic and ANN. International Journal of Engineering Research in Africa, 19, 2015, pp. 130-137.
[9]. D. Sobya, P S Chakraborty and Dulal Krishna Mandal. Design and development of IoT based residential automation security system with bluetooth technology. International Journal of Application or Innovation in Engineering and Management, 6(6), 2017, pp. 62-72.
[10]. S. Scott-Hayward, S. Natarajan and S. Sezer. A survey of security in software defined networks. Communications Surveys and Tutorials IEEE, 18(1), 2017, pp. 623-654.
[11]. D. Sobya, Arvind Kumar and Vicky Kumar. Smart IoT based energy monitoring and controlling household appliances. International Innovative Research Journal of Engineering and Technology, 2, 2017, pp. 94-97.
[12]. S. Nallusamy, G.B. Dinagaraj, K. Balakannan and S. Satheesh. Sustainable green lean manufacturing practices in small scale industries-A case study. International Journal of Applied Engineering Research, 10(62), 2015, pp. 143-146.
[13]. D. Sobya, R. Varshni and P. Albinia. MEMS based hand gesture wheel chair movement control with emergency alert. International Innovative Research Journal of Engineering and Technology, 2, 2017, pp. 90-93.
[14]. Khurshid, Zhou, Caesar and Godfrey. Veriflow-Verifying network-wide invariants in real time. ACM SIGCOMM Computer Communication Review, 42(4), 2012, pp. 467-472.
[15]. D. Sobya. Data compression analysis of rocket engines with vector quantization based on FCM algorithm. International Journal of Engineering Research in Africa, 22, 2016, pp. 135-140.
[16]. Y. Cui et al. SD-AntiDDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 68, 2016, pp. 65-79.
[17]. D. Sobya. Lab view based multi-input fuzzy logic controller of DC motor speed control. International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(1), 2015, pp. 55-60.
[18]. C. Hung, W. Peng and W. Lee. Energy aware set covering approaches for approximate data collection in wireless sensor networks. IEEE Transactions on Knowledge and Data Engineering, 24(11), 2012, pp.1993-2007.
[19]. D. Sobya. Discrete wavelet transform for image compression and reconstruction via VLSI. International Research Journal in Advanced Engineering and Technology, 1(1), 2015, pp. 31-35.
[20]. A. Lakshman and P. Malik. Cassandra: A decentralized structured storage system. ACM SIGOPS Operating Systems Review, 44(2), 2010, pp. 35-40.
[21]. D. Sobya. Design and execution of hybrid fuzzy controller for speed regulation of brushless DC motor. International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(1), 2015, pp. 61-68.
[22]. J. Lee, W. Chung and E. Kim. A new kernelized approach to wireless sensor network localization, Information Science, 243(10), 2013, pp. 20-38.
[23]. D. Sobya, SK. Muruganantham, S. Nallusamy and P.S. Chakraborty. Development of IoT model for public distribution method in fair price shop. International Journal of Computer Engineering and Technology, 9(3), 2018, pp. 270-278.
[24]. T. Kiravuo, M. Sarela and J. Manner. A survey of ethernet LAN security. Communications Surveys and Tutorials IEEE, 15(3), 2013, pp. 1477-1491.
[25]. D. Sobya. Design and implementation of FPGA based wave-pipelining for digital signal processing circuits. International Research Journal in Advanced Engineering and Technology, 1(2), 2015, pp. 36-42.
[26]. M. Saravanakumar, D. Sobya and B. Sathis kumar. Design and development of new technique for testing of field programmable gate arrays. International Journal of Research in Mechanical, Mechatronics and Automobile Engineering, 1(4), 2016, pp. 139-147.
[27]. D. Sobya. Data Compression Analysis of Rocket Engines with Vector Quantization Based on FCM Algorithm. International Journal of Engineering Research in Africa, 22, 2016, pp. 135-140.