IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Novel Multilayered System to Detect Malicious Attacks in Software Defined Networks

[1]Bose S, [2]Yukesh T, [2]Hariharan E U, [2]Kokul M, [3]Logeswari G

[1] Professor,[2] UG Student,[3]Research Scholar

[1,2,3] Department of Computer Science and Engineering,

[1,2,3] Anna University, Chennai, India

Abstract: The ubiquitous use of smart phone applications, development of an appropriate virtualization techniques and improvements in the innovation of cloud based decentralized network infrastructure have all resulted in the use of Software-Defined Networks for both wired and wireless applications. Network security can be dramatically improved by using standards-based software abstraction between the network control plane and the underlying data forwarding plane. In this paper, a novel multistage system to secure SDN against malicious attack is proposed. To securely manage communication, security policies can be set and applied at a fine grained level using context associated with flows, such as location, routing information, services requested, and securely labels associated with switches and controllers. This can help detect different types of attack flows, allowing varied dangers in an environment to be countered. The proposed system provides excellent results in terms of packet loss, delay and throughput.

***Index Terms* - Intrusion Detection System, Software Defined Networks, Ad-hoc On-demand Distance Vector Protocol, Neighbor Node Selection.**

I. Introduction

An Intrusion Detection System (IDS) is a system which monitors network traffic to detect suspicious activities and to generate alerts when they are detected. This type of security system collects data and information from various network sources and systems. The data collected is then analyzed to detect if an activity may constitute an intrusion or attack on the system and also helps system administrators and computer systems to prepare and deal with attacks or intrusions aimed at their network(s). Intrusion detection systems are used to identify anomalies before hackers can make any or a considerable amount of damage to a network. Intrusion Detection systems can be divided into two categories: host-based and network-based. This categorization is done based on the source of information.

The ubiquitous use of smart phone applications, development of an appropriate virtualization techniques, and improvements in the innovation of cloud-based decentralized network infrastructure have all resulted in use of software-defined networks for both wired and wireless applications. Network security can be dramatically improved by using standards-based software abstraction between the network control plane and the underlying data forwarding plane. In this paper, a novel multistage system to secure SDN against malicious attacks is proposed. To securely manage communication, security policies can be set and applied at a fine-grained level using context associated with flows, such as location, routing information, services requested, and security labels associated with switches and controllers. This can help detect different types of attack flows, allowing varied dangers in an environment to be countered. The proposed system provides excellent results in terms of packet loss, delay and throughput.

As networks expand in size and complexity, they pose greater administrative and management challenges. Increasingly, current networks are highly heterogeneous with many different devices, from small sensors and appliances to network devices such as routers to many different clients and servers and peripherals. Furthermore, these devices use different network technologies such as fixed, wireless and mobile networks. In such a complex heterogeneous environment, management of network devices (such as switches and routers), the mobility of users and devices, the dynamic variation in networks (due to failure of devices and network links), as well as the dramatic increase in security attacks are posing serious challenges. Software Defined Networks (SDN) offer a promising approach to meeting some of these challenges. SDN is rapidly emerging as a disruptive technology, poised to change communication networks in much the same way cloud computing has changed the "computer" world.

SDN is altering the texture of modern networking, moving away from the current control protocols dominant in the TCP/IP Internet stack, towards something more flexible and programmable. It has the potential to change the way networking is conducted, by enabling devices that are open and controllable by external software. In the control plane, the controller will be affected by DDoS attackers. Initiation of DDoS attacks in the OpenFlow switch - enabled controller will generate a vast amount of traffic in a short duration. On the other hand, a large number of unmatched flows is sent to the controller; thus, processing a legitimate flow request is not possible. The design of a lightweight DDoS attack solution is required for a multicontroller scenario because mobile devices, SDN controllers and switches are resource-constrained. A host location hijacking attack occurs by hijacking the host location. However, this attack is controlled by an SDN controller that evaluates the host location by examining the packet-in messages.

IP address spoofing or IP spoofing is the creation of Internet Protocol packets with a false source IP address, for the purpose of impersonating another computing system. Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program. Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation. This attack type is considered a major problem in web security. The objective of this research is to improve the security in Software Defined Network. The policy driven security architecture for securing end to end services across multiple SDN domains is proposed.

II. RELATED WORKS

Liao et al. [1] presented a variety of intrusion detection systems that were routinely used to monitor hostile activity. These systems can be installed at critical places throughout a network to analyze traffic flows, or at particular hosts or devices to monitor inbound and outbound packets from a device. Signature-based systems that recognize wrong traffic patterns and anomaly-based systems that detect departures from a model of expected normal traffic, both of which use machine learning techniques, are the most well-known IDSs. Signature-based intrusion detection systems define a set of attack patterns and a pattern similarity criterion that triggers an alarm. In order to discover patterns that depart from usual activity, anomaly-based intrusion detection systems measure the current condition of network traffic [2].

[3] provides an example of how data aggregation and traffic profile gathering might be used in the SDN controller. The authors collect network traffic parameters using the OpenFlow and sFlow protocols. Aggregation of network traffic parameters entails sending requests to network devices and getting network data on a regular basis from the SDN driver, which is closely related to packet forwarding. Marek et al. [4] presented a systematic solution that takes advantage of SDNs' intrinsic features and uses data mining to detect and classify harmful flows in the SDN data plane to protect SDNs from attackers' operations. The system's architecture and mechanics was discussed, with a focus on flow rule generation and classification.

An SDN-enabled deep-learning-driven framework [5] for threat detection in an IoT environment is proposed. For successful threat identification, the Cuda-deep neural network, gated recurrent unit (Cu- DNNGRU), and Cuda-bidirectional long short-term memory (Cu-BLSTM) classifiers are used. To demonstrate the unbiasedness of the results, 10-fold cross-validation method is used. Jayasri et al. [6] presented a detailed survey machine learning classification techniques which are commonly used to detect intrusions in the network. The authors have implemented and compared various machine learning algorithms such as Naive Bayes, and k-means clustering.

III. PROPOSED WORK

In this section, the architecture of the proposed Intrusion Detection System is presented in Fig. 1

3.1 Network Construction flow:

The first challenge is how to overcome the environment variations and reflect the status of the sensor nodes. In a harsh environment such as the intertidal area, the status of sensor nodes deployed for monitoring temperature and sea creatures are impacted by the tide, sea waves and the sea wind. Sensor nodes may change between above water and under water due to the change of the tidal level, bringing about variations in link quality and end-to-end delay. The second challenge is how to combine several factors together into the metric so as to achieve a better performance. Generally, a good routing metric should help to select the next hop which is with the best link quality, the shortest end-to-end delay and the highest residual energy. The last challenge is to balance the energy consumption among the sensor nodes so as to prolong the lifetime of each sensor node. Sensor nodes with low energy die quickly if the energy consumption is unbalanced, leading to a short lifetime and poor network performance. The steps involved in network construction flow is pictorially presented in Fig. 2

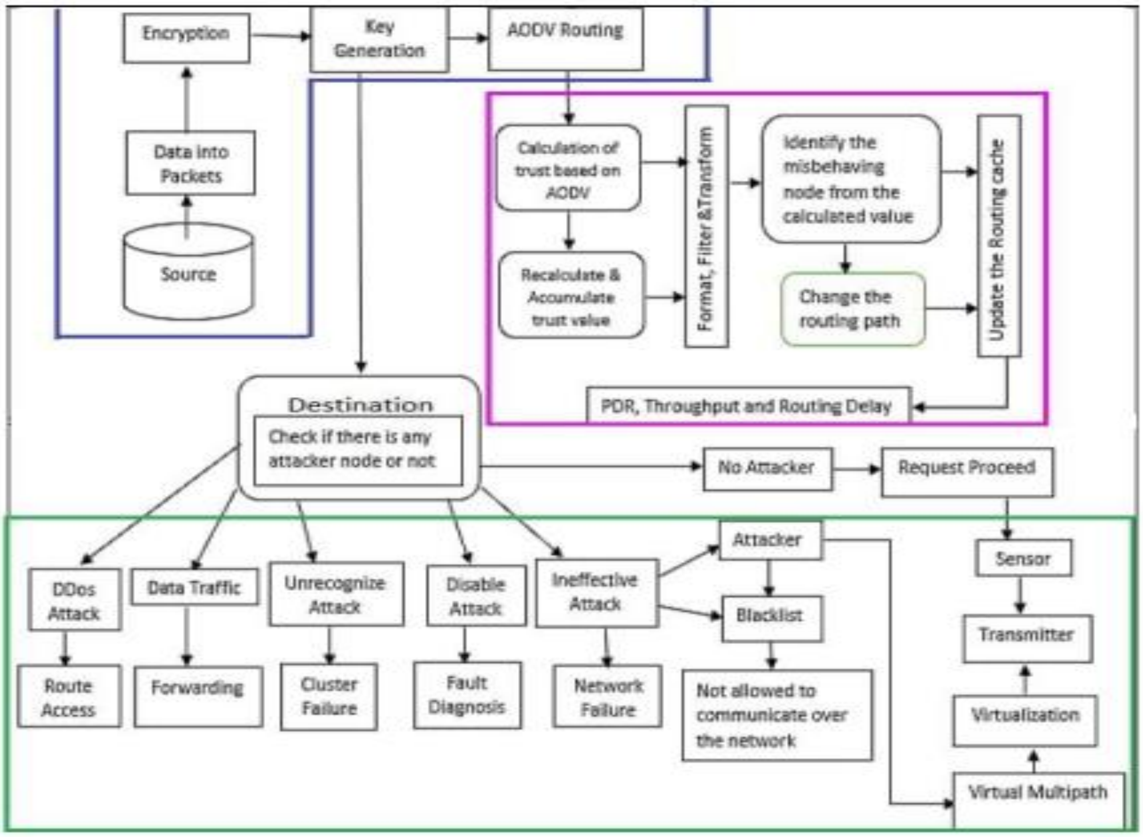

Fig. 1Proposed Intrusion Detection System

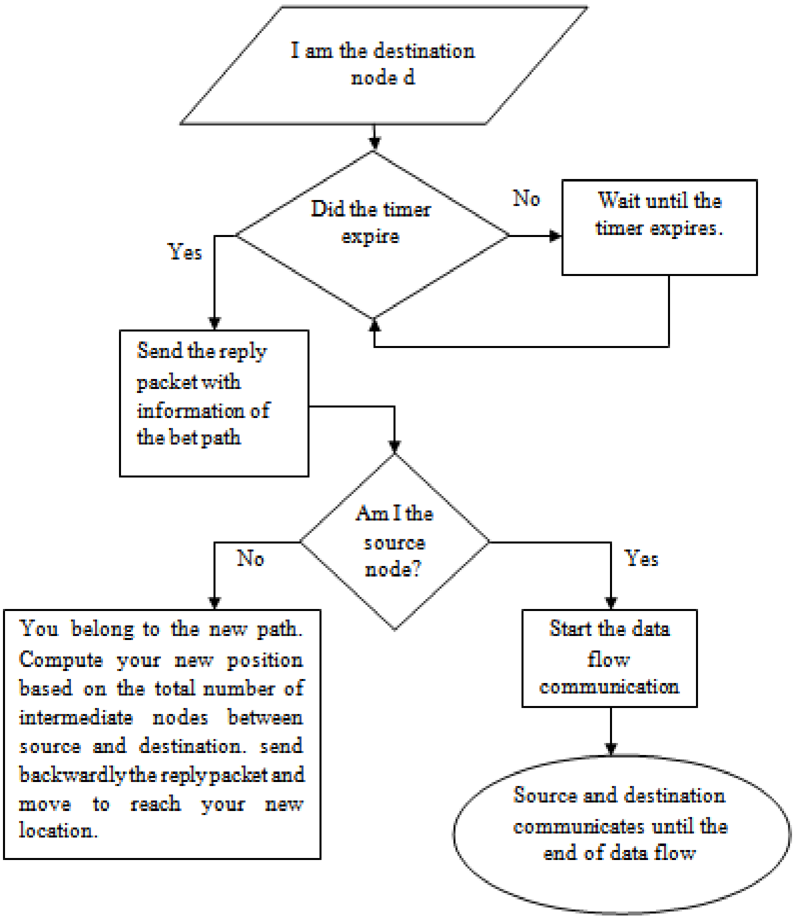
I am the destination node d
Did the timer expire
No
Wait until the timer expires.
Yes
Send the reply packet with information of the bet path
Am I the source node?
No
Yes
You belong to the new path. Compute your new position based on the total number of intermediate nodes between source and destination. send backwardly the reply packet and move to reach your new location.
Start the data flow communication
Source and destination communicates until the end of data flow

Fig 2: Network construction flow

3.2 AODV Protocol:

AODV protocol is extended with a drop factor that induces a randomness feature to result in Randomized Ad-Hoc On-Demand Routing (R-AODV) protocol. During the route discovery process, every intermediary or router node between the source and the destination nodes makes a decision to either broadcast/forward the RREQ packet further towards the destination or drop it. Before forwarding a RREQ packet, every node computes the drop factor which is a function of the inverse of the number of hop counts traversed by the RREQ packet. This drop factor lies in the range of 0 to 1. Also, the node generates a random number from 0 to 1. If this random number is higher than the drop factor, the node forwards the RREQ packet. Otherwise, the RREQ packet is dropped. Dropping of RREQ packets does not necessarily result in a new route discovery process by the source node. This is due to the fact that the original broadcast by the source node results in multiple RREQ packets via the neighbors and this diff- fusing wave results quickly in a large number of RREQ packets traversing the network in search of the destination. A major proportion of these packets are redundant due to the fact that in the ideal case, a single RREQ packet can find the best route. Also, a number of these packets diffusing in directions away from the destination shall eventually timeout. Hence, in AODV, the aim is to minimize these redundant RREQ packets, or alternatively, drop as much as possible of these redundant RREQ packets. The drop policy is conservative and its value becomes lesser with higher number of hops. In AODV, the dropping of redundant RREQ packets reduces a proportion of RREQ packets that shall never reach the destination node, resulting in a decrease of network congestion. Hence, the ratio of the number of packets received by the nodes to the number of packets sent by the nodes, namely, throughput, should be higher in R-AODV compared to AODV. Nonetheless, the main differences between connection-oriented, circuit-switched routing and connectionless packet-switched routing come not in the path selection mechanism, but rather in the actions that must be taken when a connection is set up, or torn down, from source to destination

Algorithm 1: AODV Protocol

```
Step 1: One node in the path is connected to the source
Step 2: The other node link in the path is connected to the destination.
Step 3: For all i, the i and i−1st link in the path are connected to the same node
Step 4: For the least cost path, the sum of the cost of the links on the path is the minimum
        over all possible paths between the source and destination.
Step 5: The network topology and all link costs are known, i.e., available as input to the link
        state algorithm
Step 6: c(i,j): link cost from node i to node j. If nodes i and j are not directly connected, then
        c(i,j) = infty. We will assume for simplicity that c(i,j) equals c(j,i).
Step 7: D(v): the cost of path from the source node to destination v that has currently (as of
        this iteration of the algorithm) the least cost.
Step 8: p(v): previous node (neighbor of v) along current least cost path from source to v
Step 9: N: set of nodes whose shortest path from the source is definitively known
Step 10: The call setup is blocked and another path must be attempted.
```

3.3 Neighbor Node selection:

Each node updates the route score for each of its neighbors and finds out the best score. After several iterations, the scores are completely updated and the neighbor with the best route score is then chosen as the parent node to forward sensed data. The routing paths are determined when all the sensor nodes update their route scores.

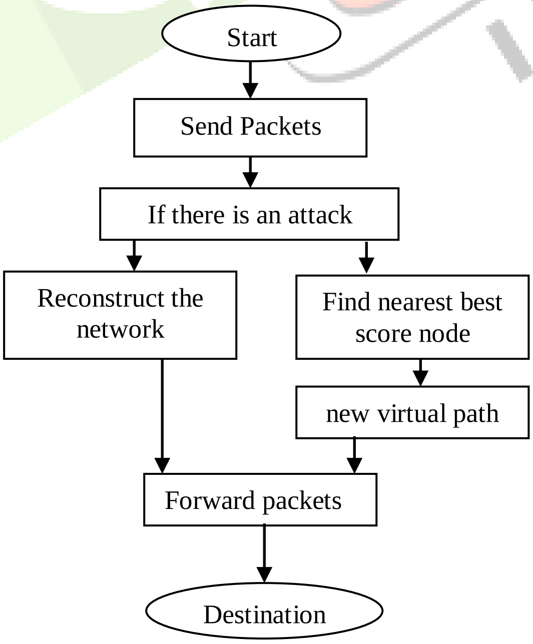

Fig. 3 Neighbor Node Selection

Algorithm 2 : Neighbor Node selection

Step 1: An algorithm selects n forwarding nodes in the worst case, The new sender-based algorithm results in fewer broadcasts.

Step 2: All these interesting properties are achieved at the cost of a slight increase in end-to-end delay

Step 3: The value of n (No. of Nodes) is typically large, and it is important to bind the packet size.

Step 4: Each node schedules a broadcast for a received message if the node is selected by the sender and if it has not scheduled the same message before. Clearly, each message is broadcast once at most by a node

Step 5: To select the forwarding nodes from its neighbors Assume that NA stores all of its neighbor's IDs and locations in an array of length n, where n is the number of neighbors

Step 6: Routing of nodes to avoid end to end delay and increase energy efficiency.

Step 7: Co- Integration analysis and Best subset node selection

Step 8: Virtualization is operated if there is an attack on the nodes and delay in transferring the packets.

3.4 Inter-domain Security:

Communications with multiple analyse the performance characteristics of our architecture as well as discuss how our architecture is able to counteract various security attacks. The dynamic security policy based approach and the distribution of corresponding security capabilities intelligently as a service layer that enable flow based security enforcement and protection of multitude of network devices against attacks are important contributions of this paper. These capabilities introduce new security threats and attack surfaces, which do not exist in traditional networks. Ironically, the closed nature of network switches together with the heterogeneity of vendor software and integrated control functions previously offered natural layers of defense in traditional networks.

Algorithm 3 : Inter-domain Security

```
Input:
Attack flow: a ; Target: d

if n node(a) > 1 then
new Node <-- new vNode();
vNetwork.node(newNode);
vNetwork.path(d,newNode);
endif
```

IV. RESULTS AND DISCUSSION

The performance of any system needs to be evaluated on certain criteria, these criteria then decide the basis of performance of any system. Such parameters are known as performance metrics. The following performance metrics are considered for evaluation of network topologies:

1) Throughput: Network throughput refers to how much data can be transferred from source to destination within a given time frame. Throughput measures how many packets arrive at their destinations successfully. For the most part, throughput capacity is measured in bits per second, but it can also be measured in data per second.

Throughput = (Sum of no. of Successful packet x Average packet size) / Total time

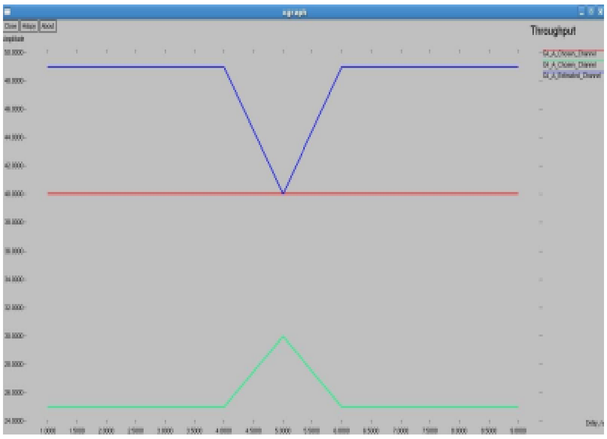

Fig 4: Throughout

2) Delay: Network delay is a design and performance characteristic of a telecommunications network. It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. It is typically measured in multiples or fractions of a second.

Delay = Transmission delay + Propagation delay + Queuing delay + Processing delay

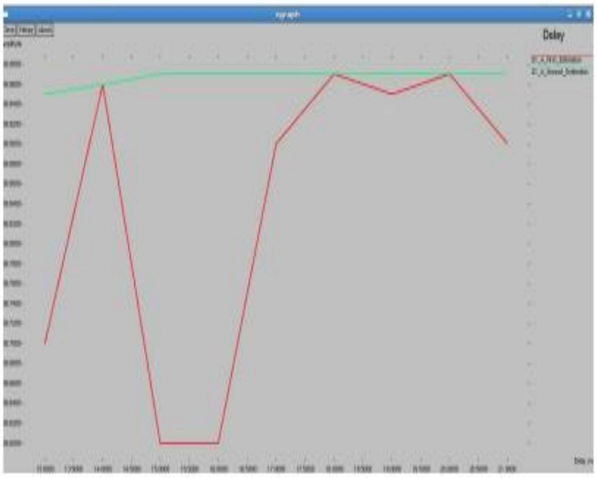

Fig 5: Delay

3) Pack Loss on Traffic: Packet Loss is defined as "the rate of loss of packets in the network". The packet loss by each would be virtualize with respect to nearby nodes.

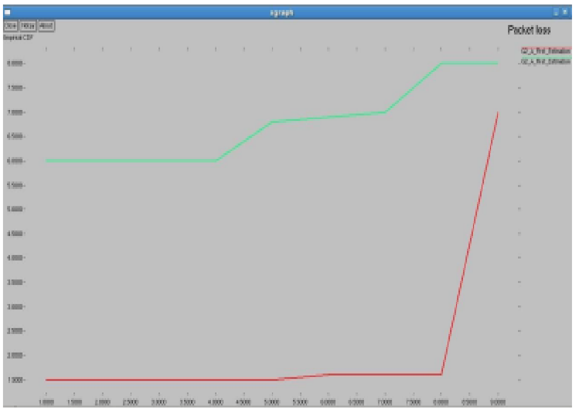

Fig 6: Packet Loss

V. CONCLUSION

Software Defined Networks as an emerging technology brings innovation into the networking with the decoupling of control and data plane, removing proprietary in the network architecture to open and programmable network. The main goal of the research is to improve the security in Software Defined Network. The policy driven security architecture for securing end to end services across multiple SDN domains is proposed. The proposed multilayered system using virtualization identifies various types of attacks. The proposed system tries to solve various security issues.

REFERENCES

[1] Liao, H.J. Richard Lin, C.H., Lin Y.C., Tung K.Y. 2013. Intrusion detection system: A comprehensive review. J. Netw. Comput. Appl. 36:16–24.

[2] Umer, M.F. Sher, M. Bi, Y. 2017. Flow-based intrusion detection: Techniques and challenges. Comput. Secur. 70:238–254.

[3] Giotis, K. Argyropoulos, C. Androulidakis, G. Kalogeras, D. Maglaris, V. 2014. Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Comput. Netw. 62:122–136.

[4] Amanowicz, Marek, and Damian Jankowski. 2021. Detection and Classification of Malicious Flows in Software-Defined Networks Using Data Mining Techniques. Sensors (Basel, Switzerland) 21(9): 2972.

[5] Javeed, D Gao, T. Khan, M.T. Ahmad, I. 2021. A Hybrid Deep Learning-Driven SDN Enabled Mechanism for Secure Communication in Internet of Things (IoT). Sensors. 21:4884.

[6] Jayasri, P. Atchaya, A. Sanfeeya Parveen, M. Ramaprasath, J. 2021. Intrusion Detection System in Software Defined Networks using Machine Learning Approach. International Journal of Advanced Engineering Research and Science. 8(4):135-142.

[7] Kim, T Lee, T. Kim, K. Yeh, H. and Hong, M. 2013. An efficient packet processing protocol based on exchanging messages between switches and controller in OpenFlow networks. 10th International Conference and Expo on Emerging Technologies for a Smarter World (CEWIT).1-5.

[8] Auer, G. Giannini, V. Desset, C. Godor, I. Skillermark, P. Olsson, M. 2011. How much energy is needed to run a wireless network. IEEE Wireless Communications. 18: 40-49.

[9] Neokosmidis, I. Rokkas, T. Paglierani, P. Meani, C. Nasr, K.M. Moessner, K. 2018. Techno Economic Assessment of Immersive Video Services in 5G Converged Optical/Wireless Networks. Optical Fiber Communications Conference and Exposition (OFC). 1-3.

[10] Poongodi, M. Bose, S. 2015. A Novel Intrusion Detection System Based on Trust Evaluation to Defend Against DDoS Attack in MANET. Arab J Sci Eng 40: 3583–3594.

[11] Nguyen, V.G. Brunstrom, A. Grinnemo, K.J and Taheri, J. 2018. 5G Mobile Networks: Requirements, Enabling Technologies, and Research Activities. A Comprehensive Guide to 5G Security. 31-57.

[12] Zhang, Z. Gao, Y. Liu, Y. and Li, Z. 2018. Performance evaluation of shortened transmission time interval in LTE networks. Wireless Communications and Networking Conference (WCNC). 1-5.

[13] Belkhir, L. and Elmeligi, A. 2018. Assessing ICT global emissions footprint: Trends to 2040 & recommendations. Journal of Cleaner Production. 177:448-463.

[14] Aneetha, A S. Indhu ,S, Bose S.2013. Hybrid Network Intrusion Detection System Using Expert Rule Based Approach. The Second International Conference on Computational Science, Engineering and Information Technology. 22.

[15] Aktas, A.Z. 2017. Could energy hamper future developments in information and communication technologies (ICT) and knowledge engineering. Renewable and Sustainable Energy Reviews.

[16] Lähdekorpi, M. Hronec, M. Jolma, P. and Moilanen, J. 2017. Energy efficiency of 5G mobile networks with base station sleep modes. Standards for Communications and Networking (CSCN). 163-168.