iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3366

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Improving Quality of Service through SDN for Mobile Networks

Divya M[1], Kavin Mathi G[2], Monisha K V[3], Sridevi P M[4], Thilagam K[5]
[1, 2, 3] *UG Student, Department of ECE, Velammal Engineering College*
[4] *Associate professor, Department of ECE, Velammal Engineering College*

Abstract: ***In the past decade, mobile devices and its application have experienced a tremendous growth, and users are in need of higher data rates and better-quality services every year. Connection between users and services in mobile networks has to pass through required set of middleboxes. The complex routing is one serious problem. In this paper, software defined network is used which enables policy based aware routing in mobile networks. The policy aware routing with trust evaluation algorithm is proposed. The main objective is to steer traffic flows to maximize the total amount of traffic and quality of service constraints. In the simulation scenario, the existing work is compared with proposed work. It is inferred that parameters like packet delivery, throughput, energy consumption, latency performance can be enhanced compared to conventional method***

I. INTRODUCTION

3G uses packet switching rather than circuit switching because of demands from the users. Mobile broadband technologies are now an important part of the communication infrastructure even for most of the developing world. The QoS issues related to the deployment of multimedia services in cellular technologies are then considered and analyzed through the inclusion of the communication technology and application related parameters along with number of users in QoS evaluations discussed [1]. Providing high quality is very challenging. Author's used multilevel broker which will have information about available network resources thus guarantees the quality of service [2,3]. The mobile network has to achieve end to end QoS guarantee which is provided by cross layer design which decompose function into modular components in OSI layer where it achieves high data rate, less delay and user fairness for next generation wireless networks was discussed [3]. The Wideband Code Division Multiple Access was upgraded to High Speed Packet Access and then to 4G which serves more number of users and it provides high data rate for new applications. Each middlebox is deployed as a separate device, these resources cannot be amortized across applications even though their workloads offer natural opportunities to do so. Consolidated middlebox architecture which systematically explores opportunities for consolidation and provides new opportunities for resource savings via application multiplexing, software reuse, and spatial distribution was discussed [4]. Traditional network architectures are ill-suited to meet the requirements of today's end users. In SDN, the control and data planes are decoupled. SDN is dynamic and flexible network architecture that provides network reliability and security as it is centrally controlled using software applications [5]. SDN simplifies network devices. Network operators can programmatically configure this simplified network rather having thousands of lines of configurations [6,10]. The growth of a middleware framework which support the operation of adaptive Wireless Sensor Networks applications with real-time application and dependability requirements. Middleware need to possess attributes of availability, reliability, safety, integrity and maintainability in order to fulfill the parameters of real time applications. Dependability objectives are achieved by adaption process so that middleware that support dependability and timeliness requirements was proposed which meets the attributes effectively [7]. The complex routing is one of the serious problem in wireless networks so they proposed both offline planning and online routing problem in SDN. The offline planning is one where demands are specified and the aim is to identify whether there is enough capacity in the network to handle demands. In online routing, flow request is given one at a time to steer the flow to maximize the amount of traffic accepted over time [8]. Mobile data is continuing to grow exponentially and is taking up a larger portion of total Internet traffic in recent years. The latest 4G LTE network uses an all-IP evolved packet core (EPC), but the network structure is still hidden from the public Internet, and mobile traffic from/to a mobile user equipment (UE) must pass through special NE including nodes, serving gateways, packet data network gate-way (PGW), and certain middleboxes in a specific manner. So here they have proposed a policy aware routing with log competitive algorithm to improve the quality of service [10].

As demands on the data center rapidly grow, so too must the network also grow. However, the network also become complex with the addition of hundreds or thousands of network devices that must be configured and managed. IT has also relied on link oversubscription to scale the network, based on predictable traffic patterns;

But, in today's virtualized data centers, traffic patterns are incredibly dynamic and therefore unpredictable. To overcome all these problem, we go for software defined networking with virtualization of nodes is chosen.

SDN decouples the data and control planes, and routing decisions are made in a centralized manner rather than hop-by-hop. For each traffic flow, the controller not only selects the best NE, but can also specify the best route to take. This gives SDN the ability to steer traffic in fine granularity to enforce policy-based routing, meet QoS requirements of various applications, and perform network-wide resource optimizations as well. Therefore, SDN becomes a promising candidate to enhance mobile networks.

The main functional requirements are

The first requirement is designated by message forwarding. It is about the successful delivery of messages to final destinations in spite of the eventual disruption originated by handovers (or handoffs).

These handovers, traditionally justified by node mobility, in the future network environment uses dynamic selection of an alternative Network Attachment Point (NAP) which offer higher connectivity quality than the one being used.

The second requirement is the route update that characterizes how fast a new routing path is propagated across the network, including the mobility agents or correspondent nodes, after a node has moved to other NAP. Ideally, the packets should be delivered with success to their final destinations in spite of these being mobile terminals faster

The third requirement is concerned with how efficiently the technology manages handovers, minimizing packet loss, network overhead and delay. In this way, the handover process should not disrupt the quality associated to traffic flows used by the mobile terminal.

The fourth requirement is related with security. The mobility management solution should not introduce any new security vulnerabilities. As an example, the client privacy should be always guaranteed

Our contributions are

A. Policy aware routing to maximize total traffic accepted over time to achieve better Quality of Service with the help of software defined network

B. Trust Evaluation algorithm ensures that every communicating nodes are trustworthy during authorization, authentication. This makes the security services more reliable and robust. Moreover, it will improve the system performance by increasing the cooperation among nodes. To evaluate the trustworthiness of the neighbors, a node not only monitors their explicit observations but also communicate with other nodes to exchange their opinions.

C. Aware routing -Trust Evaluation Algorithm ensures that maximum data is transmitted over time and nodes are trustworthy during communication

II. DESIGN MOTIVATION

In a SDN, Packets are sent to the nodes from a controller, an application which is running on a server at different place, and the nodes query the controller for assistance and to provide with information about traffic which they are handling.

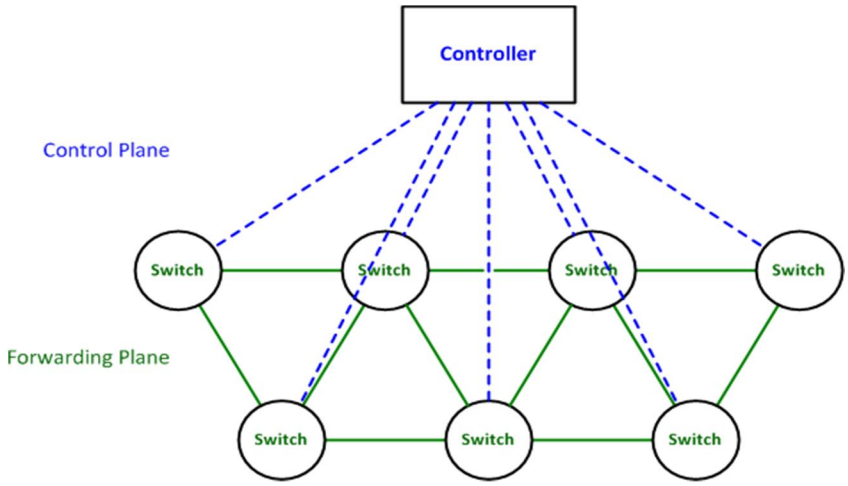
With the help of SDN, the network manager can change any node's rules which is necessary at time like -- prioritizing, de-prioritizing or even blocking specific types of packets with a very granular level of control.

In SDN, a network administrator can control traffic from a central control console without need of touching every switch and can deliver service. The key technologies for SDN are separation of planes, network virtualization and programmability.

At first SDN merely focuses on separation of data plane and control plane, which makes decision about how packets should flow through the network.

When a packet reaches the node, it decided where to forward the packet. The node sends every packet going to the same from a destination along the same path and treats all the packets the exact same way.

Routing in networks using SDN

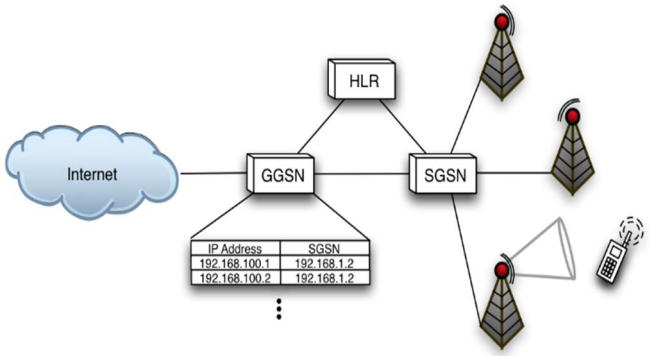


A. Design Goals

1) Flexible policy enforcement through SDN. Fine-grained control should be exercised to steer data flows through NE deployed throughout the network.

2) Providing truly end-to-end QoS guarantees. QoS optimization should be pushed to both ends of data flows rather than on a hop-by-hop basis. Competitive network resource optimization has been carried out in a distributed way and settled at sub-optimal heuristic solutions, yet it can be further explored in a centralized manner.

3) The trust evaluation algorithm attains confidentiality and authentication of packets in routing layer and flexible enough to trade security for energy consumption. It is also attack tolerant to facilitate the network to resist attacks and device compromises besides assisting the network to heal itself by detecting and recognizing and eliminating the source of attacks



B. Algorithm

1) Existing Method

a) Policy Aware Routing: A major objective of mobile traffic steering is to maximize the total amount of traffic accepted over time in a policy-aware manner without violating any node/link capacity, operational budget, or QoS constraints. In this section, we formulate a variant of the well-known maximum multi-commodity flow problem and incorporate other techniques to meet policy awareness and QoS constraints was formulated. The author formulated the problem as a mixed integer programming problem. We use a binary variable xdp to indicate whether path p is chosen for flow d. When a request enters the system, it is either accepted for the entire duration and carried on a single path or is rejected.

$$\text{Maximize} \quad \alpha \triangleq \sum_{d} \sum_{p \in \mathcal{P}_d} h_d \tau_d x_{dp} \qquad \text{(1a)}$$

$$\text{Subject to} \sum x_{dp} \leq 1, \quad \forall d \qquad \text{(1b)}$$

$$\sum_{d|t\in[\tau_d^s,\tau_d^f]}\sum_{p\in\mathcal{P}_d|e\in p}\sum_{i|e\in p^{(i)}}\gamma_d^{(i)}h_d x_{dp}\le c_e,\quad \forall e,\forall t \tag{1c}$$

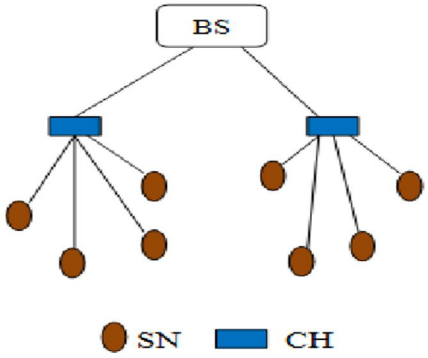
$$\sum_{d|t\in[\tau_d^s,\tau_d^f]}\sum_{p\in\mathcal{P}_d}\sum_{i}\sum_{e\in p^{(i)}}b_{et}\gamma_d^{(i)}h_d x_{dp}\le B_t,\quad \forall t \tag{1d}$$

Constraint(1a) seeks to maximize the total accepted traffic over time. Constraint(1b) ensures that each flow is allocated at most once. Constraint(1c) ensures budget constraint. Constraint(1d) ensures QoS enforcing constraints.

C. Proposed Method

1) *Aware Routing-Trust Evaluation Algorithm (Artea):* Trust management ensures that every communicating nodes are trustworthy during authorization, authentication. The methods for attaining trust information and defining each node's trustworthiness are referred to as trust models. A trust model is mostly used for higher layer decisions such as routing and data aggregation, cluster head election and key distribution. Even though there are lots of designs in trusty models, their implementation has attracted nearly no attention. In Cluster wireless sensor networks (LEACH, EEHC, EC), clustering algorithms can efficiently improve the network scalability and throughput. In clustering algorithms, each node is bound in clusters, and within each cluster, a node with strong computing power is selected as cluster head (CH). The clustering algorithm constructs a multilevel WSN structure, after several recursive iterations. This structure enables the restriction of bandwidth consuming network operations such as flooding only to the intended clusters. Existing trust systems such as GTMS, HTMP, ATRM are failing to focus on the resource efficiency and dependability of the system. To achieve all these, need an efficient Trust Evaluation System for Wireless Sensor Networks is proposed in this paper. A weighted trust evaluation is used to detect the compromised nodes by monitoring its reported data. This paper focus on the dependable trust evaluating approach for cooperation between cluster heads. The indirect way of trusting a node is calculated by cluster head. Thus, each member in the cluster does not need to maintain the feedback from other members. This method will eliminate the possibility of a bad-contagious attack by compromised sensor nodes.

III. NETWORK ARCHITECTURE



Cluster based WSN consisting of multiple clusters, that each node in the clustered WSN model can be determined as a Cluster Head (CH) or Sensor Node (SN) or Forwarding Node (FN). Cluster Head directly interacted by their Sensor Node. Cluster Head can transmit the combined data to the central base station or the destination node (or sink node) through other Cluster Head. It is assumed that nodes are organized into clusters with the help of a proposed cluster scheme. A number of SNs are organized as a group and it is controlled by a CH. Hence, every sensor node communicates only with its CH. Let us consider the CHs and BSs are trustful and won't be compromised. Each CH provides two-way communications. One with sensor node and another with base station. BS provide multihop routing packets from SNs and CHs within their range. Based on the information obtained from the SNs, CHs compute the aggregation result and informs the information to BSs. It is important for CHs to monitor whether the information collected from the SNs are correct or not.

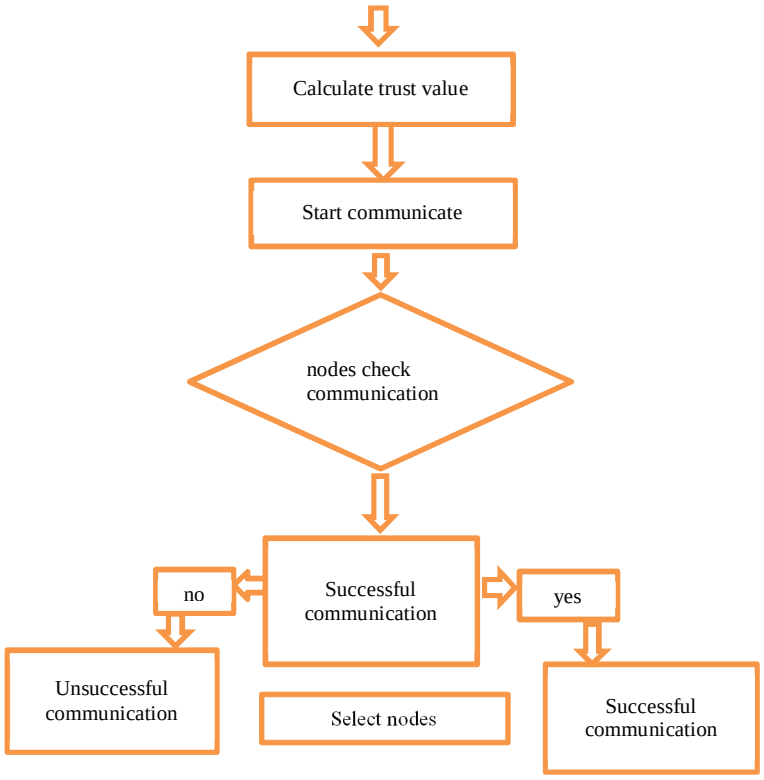
$$S_{l,m}(\Delta t)=\left[\left(\frac{10\times f_{l,m}(\Delta t)}{f_{l,m}(\Delta t)+g_{l,m}(\Delta t)}\right)\left(\frac{1}{\sqrt{g_{l,m}(\Delta t)}}\right)\right]$$

A. SN-to-SN Direct Trust

Sensor node calculates the trust value of its neighbors based on direct trust and feedback trust. Direct trust is calculated by the number of successful communication and unsuccessful communication. Let us consider node l transmits a message to cluster head b via node$m$. Node a checks whether the node m transmit the message to CH b . If node a does not listen the retransmission of the packet within a threshold time from its neighboring node m, then a will be considered as communication failure.

where Δt is a window of time as time elapses, the window adds newer experience but forgets the previous old experience. $f_{l,m}(\Delta t)$ is the total number of successful cooperation?

$g_{l,m}(\Delta t) \neq 0$ is the total number of unsuccessful interactions of node l with m during time Δt. If $f_{l,m}(\Delta t) \neq 0$ and $g_{l,m}(\Delta t) = 0$, we set $S_{l,m}(\Delta t) = 10$. When there is no interactions between node $l$and m during time Δt, the sum of $f_{l,m}(\Delta t)$ and $g_{l,m}(\Delta t)$ is 0. $S_{l,m}(\Delta t)$ is used for calculating the SN-to-SN direct trust method.



B. CH-to-SN feedback trust

WTES-WSN does not utilize a broadcast-based strategy and instead sets the indirect trust value is based on the feedback reported by the CH about a specific node. Thus, each SN does not need to share trust information with its neighbors. This action has effective reduction of the effect of malicious value, thereby reducing the networking risk in an open WSN environment. For example, if a node a wants to communicate with node m, the transmitter node checks whether it has any previous communication with the destination node during a specific time interval. If the previous communication record exists, then a makes a decision directly. Otherwise node a will send a feedback request to its Cluster Head b.

$S_{l,m}(\Delta t)$ is also considered as $D_{n,m}(\Delta t)$. It is very helpful for calculating the CH-to-SN indirect trust method. Consider that there are $(v-1)$ sensor nodes in a cluster. Within the cluster the CH ch will periodically transmit the request packet. Every SNs in the cluster will forward their trust values toward other SNs to ch . The equation of $D_{ch,m}(\Delta t)$ is defined as

$$D_{ch,m}(\Delta t) = \lceil 10 \times H(\beta(p|c,e)) \rceil \quad (2)$$

Where p denotes the posterior probabilities of binary events

(c, e). e is the amount of negative feedback towards the node m. $H(\beta(p|c,e)$ is the probability expectation value of beta distribution $\beta(p|c,e)$. $H(\beta(p|c,e) = (c+1)/(c+e+2)$.

With an increase in the number of unsuccessful interactions $1/\sqrt{g_{l,m}(\Delta t)}$ rapidly equals to 0. This feature effectively avoids sudden attacks from malicious nodes with higher accumulated trustworthiness.

C. *CH-to-CH direct trust*

The selection of CH is a very important for dependable communication. Because CH can forward the aggregated data to the central BS through CHs. In CH-to-CH communication, the direct trust value is calculated according to the number of successful and unsuccessful interactions. When a CH b wants to communicate with another CH q , it will send a feedback request to the BS. The BS periodically collects all CHs for their trust ratings on their neighbors. After receiving the results from the CHs, the BS will combine them to form an effective trust value. Thus, this mechanism can greatly reduce the network communication overhead and improve the system efficiency. For example, if a Cluster Head b wants to interact with another Cluster Head q, b initially calculates CH-to-CH direct trust for x based on past communication records with q during specific time interval. Meanwhile b sends a feedback request to the BS. After receiving the request, the BS will send a response message to b, in which q's feedback trust value is combined. Then b will combine these trusted sources into a group trust detection, after b will make a final decision based on q's group trust value. The direct trust value between Cluster Head b toward another Cluster Head q is defined as:

$$C_{b,q}(\Delta t) = \left[\left(\frac{10 \times F_{b,q}(\Delta t)}{F_{b,q}(\Delta t) + G_{b,q}(\Delta t)} \right) \left(\frac{1}{\sqrt{G_{b,q}(\Delta t)}} \right) \right] \quad (3)$$

where $G_{b,q}(\Delta t) \neq 0$. $F_{b,q}(\Delta t)$ and $G_{b,q}(\Delta t)$ are the total number of successful and unsuccessful interactions of CH b with CH q during time window Δt respectively. When $F_{b,q}(\Delta t) \neq 0$ and $G_{b,q}(\Delta t) = 0$, $C_{b,q}(\Delta t)$ is set as 10.

BS-to-CH feedback trust: Let us consider z number of CHs exists in a network. Within the cluster, the base station bswill periodically broadcast the request packet. All CHs in the network will transmit their trust values toward other CHs to bs. Similar to the previous method, enhanced beta probability density function is used to determine for BS-to-CH feedback trust.

$$L_{bs,q}(\Delta t) = \left\lceil \frac{10 \times H\left(\beta(p|d,\sigma)\right) + \overline{C_{y,q}}(\Delta t)}{2} \right\rceil$$

Where p denotes the posterior probabilities of binary events (d, σ), $d$is the positive feedback and σ is the amount of negative feedback. The probability expectation value of beta distribution function $\beta(p|d,\sigma)$ is:

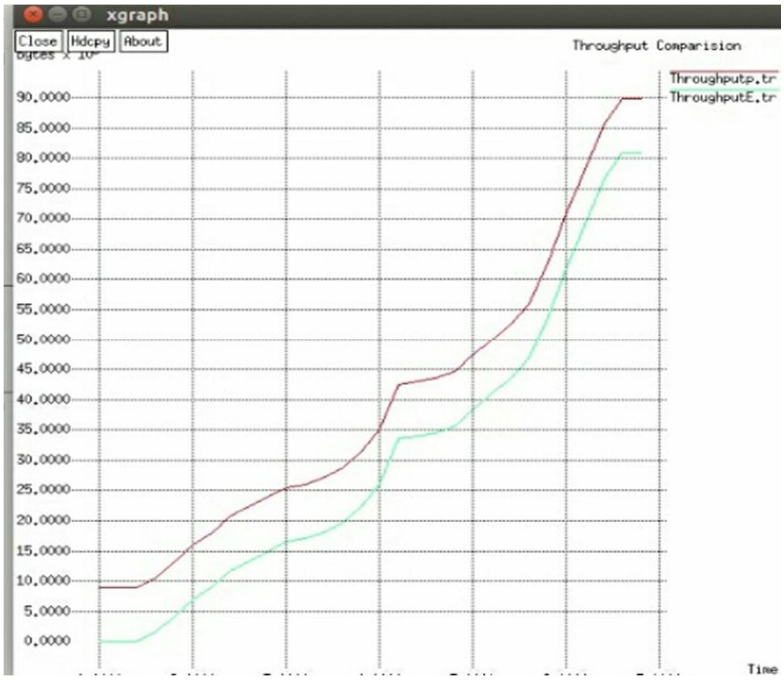
$$H\left(\beta(p|d,\sigma)\right) = \frac{d+1}{d+\sigma+2} \quad (5)$$

$\overline{C_{y,q}}$ is the average value of aggregates feedback from $(d+\sigma)$ CHs in network?

$$\overline{C_{y,q}}\ (\Delta t) = \frac{\sum_{y=1}^{d+\sigma} C_{y,q}(\Delta t)}{d+\sigma} \quad (6)$$

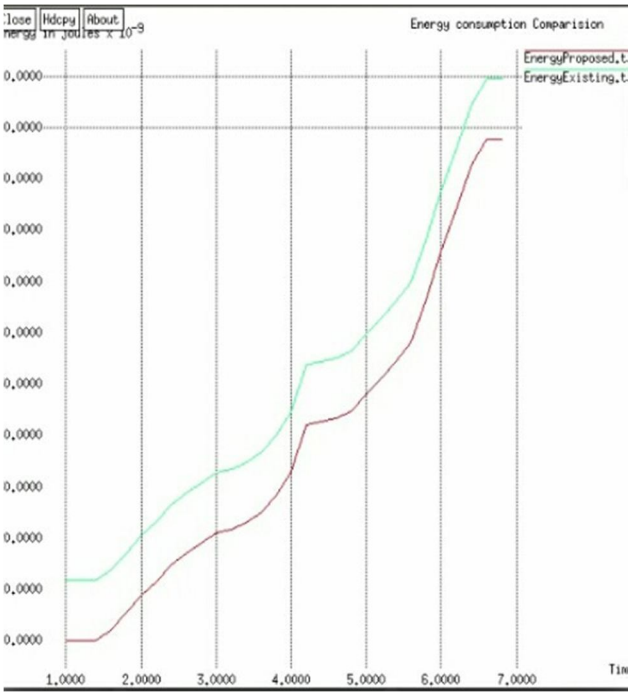
Where $C_{y,q}(\Delta t)$ is the feedback of CH y toward CH q. This technique considers the quality of each feedback$C_{y,q}(\Delta t)$ with the amount of feedback $(d+\sigma)$

IV. SIMULATION RESULT



A. Throughput Comparison

From the above simulation result shows the comparison graph. It is inferred that throughput of proposed scheme is better than existing method.

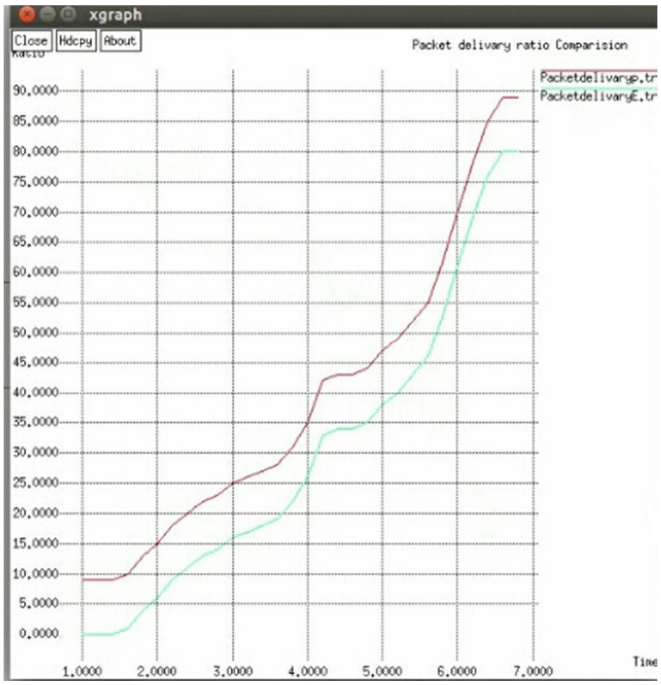


B. Energy Comparison

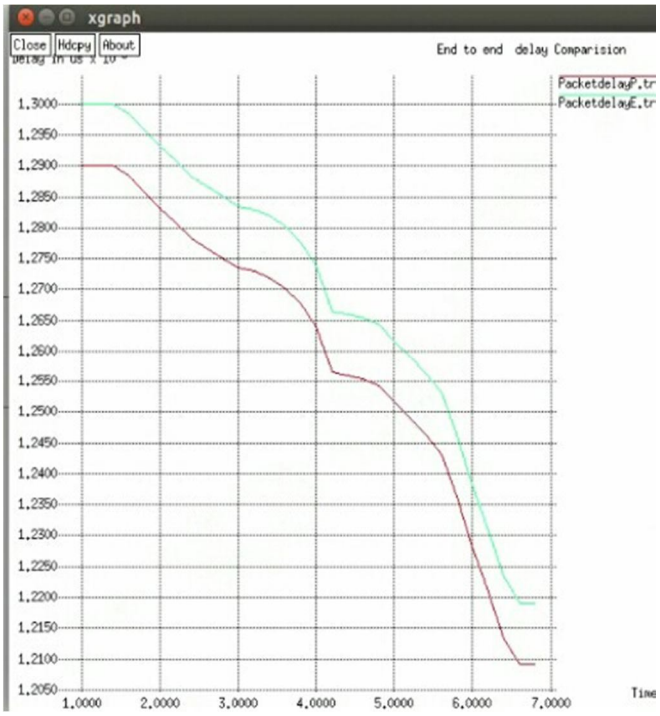
The simulation of energy consumption of both the methods were shown. It is observed that energy consumption is less compared to existing scheme.

The above graph is the simulated output for energy consumption

C. Packet Delivery Comparison



The above results show the comparison graph. It is inferred that packed delivery is higher in proposed scheme compared the conventional method for the packet delivery rate.



D. Delay Comparison

The above figure shows the comparison graph of packet delivery delay for the proposed system to existing method. It is notified that delay in the packet delivery is less compared to existing method.

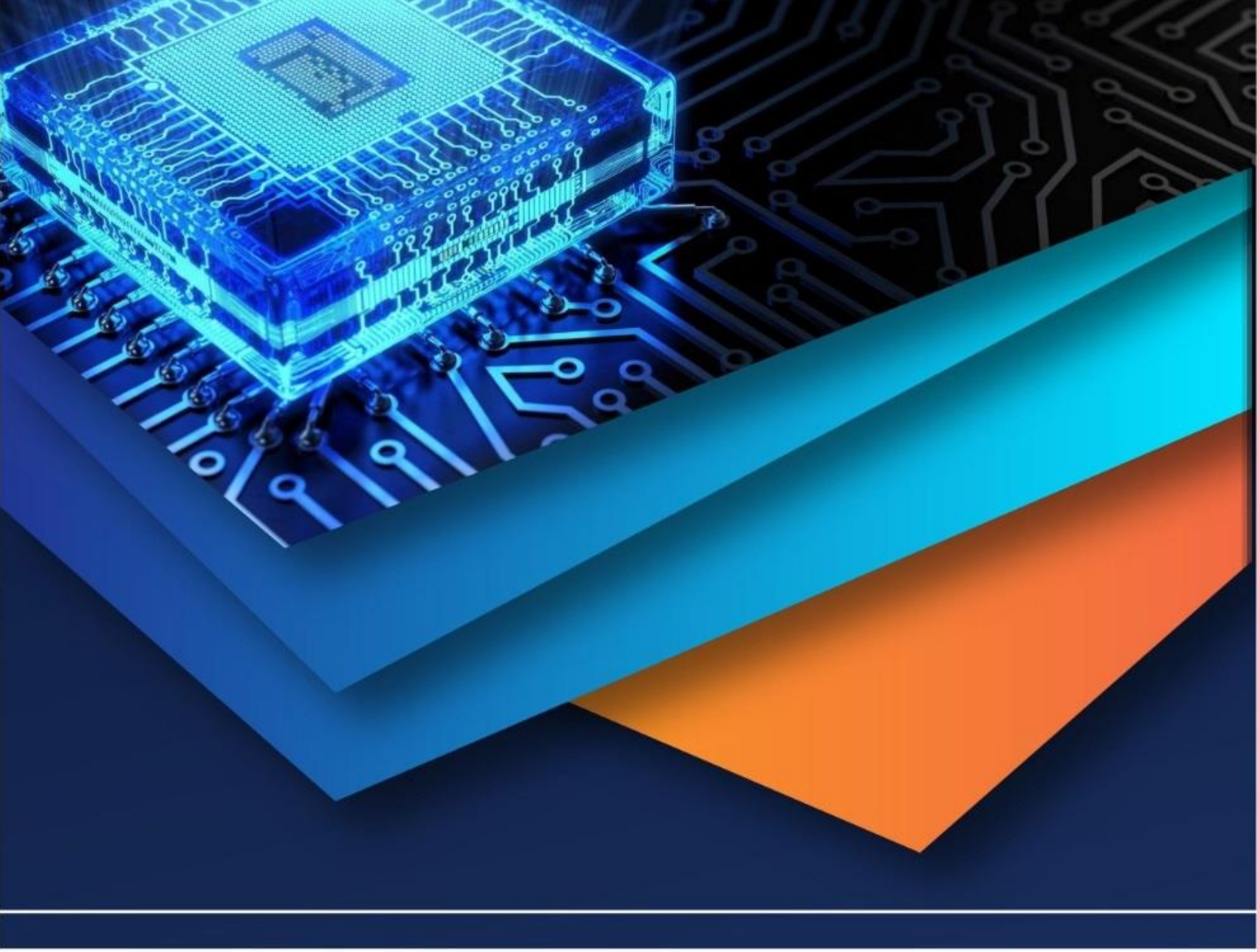
It is observed that the simulated results improved performance in energy consumption, throughput, packet delivery, latency compared to existing method.

V. CONCLUSION

Middleboxes have become ubiquitous in wide area networks. Simple routing of flows from node to node along shortest path has been replaced by policy aware paths that have to pass through middleboxes. In this paper, we reveal the infrastructure difficulties and routing problems in the current mobile networks is analyzed. In this paper we proposed an SDN-based architecture to address the potential bottlenecks and challenges of next generation mobile networking through ARTEA with software defined networking. The simulation has been performed to investigate various parameters like packet delivery and throughput which has been increased and parameters like latency and energy consumption are reduced which is better than existing method.

REFERENCES

[1] QoS Analysis and Evaluations: Improving Cellular-Based distance education Farnaz Farid, Seyed Shahrestani, and Chun Ruan School of Computing, Engineering and Mathematics University of Western Sydney, Sydney, Australia 2013
[2] Improving QoS in multi-operator cellular networks Rafael kunst, Leandro Avila, Edison Pignaton, Sergio Bampi, Juergen Rochol 2016.
[3] Cross layer based Qos improvement in cellular networks Vandhana Khare, Dr y. Madhavee Latha,Dr D. Srinivasa rao ,2015.
[4] Design and Implementation of a Consolidated Middlebox Architecture Vyas Sekar, Norbert Egi, Sylvia Ratnasamy, Michael K. Reiter, Guangyu Shi Intel Labs, UC Berekley, UNC Chapel Hill, Huawei 2012.
[5] Software defined networking: The newform for Networks, ONF WHITE PAPER 2015.
[6] Applying NFV and SDN to LTE Mobile core Gateways, the function placement problem Arsany Basta, Wolfgang Kellerer, Marco Hoffmann, Hans jochen Morpher, Klaus Hoffmann2014.
[7] Middleware support for adaptive real time applications in wireless sensor networks Josao Alves, Antonio Casimiro, and Luis Marques
[8] Traffic steering in software defined networks: planning and online routing 2014 zizhong cao, murali kodialam, T.V. Laxman
[9] Making middleboxes someone else's problem: Network processing as a cloud service in Proc. ACM SIGCOMM, 2012.
[10] Enhancing Mobile Networks with Software Defined Networking and Cloud Computing Zizhong Cao, Student Member, IEEE, Shivendra S. Panwar, Fellow, IEEE, Murali Kodialam, Member, IEEE, and T. V. Lakshman, Fellow, IEEE, ACM ,2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY