IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 2, Ser. IV (Mar - Apr 2019), PP 32-38
www.iosrjournals.org

Enhanced the Performance of VANET Network Using Clustering Based Thresholding Technique for Reliable Communication

Nidhi Saxena[1], Dr. Shilpa Sharma[2].
Ph.D. Scholar, School of Computer & System Science Jaipur National University
Associate Professor, School of Computer & System Science Jaipur National University
Corresponding Author: Nidhi Saxena

Abstract: *The current decade of technology gives the concept of intelligent transportation systems. The intelligent transportation systems need the reliable communication. For the reliability of communication in VANET network used various security and communication model. In this paper proposed the cluster based threshold function for the reliable communication. The proposed algorithm used distributed clustering technique for the region selection of mobile vehicles. The speed and path divergence set the value of threshold for the selection of new path and avoid the malicious packet from the other nodes. The malicious packets increase the traffic load and decrease the performance of VANET network. The proposed algorithm simulated in MATLAB and used urban traffic scenario for the evaluation of parameters.*

Keywords: *VANET, Clustering, Thresholding, Reliable, MATLAB, Traffic*.

Date of Submission: 10-04-2019 Date of acceptance: 25-04-2019

I. Introduction

In this paper changed the AODV steering convention for anticipation of DOS attack. The DOS assaults make a passage for source hub to goal hub for the correspondence procedure [2]. The recognition of DOS hub is extremely troublesome because the assaults of DOS in VANET arrange not diminish the execution of leaving system. For the counteractive action of assaults utilized thickness based grouping method. The thickness based grouping method covers the hub on the premise of two useful parts one is greatest bounce check and least trust tally [6-9]. The procedure of seek number measure the correspondence hit after the procedure of correspondence. The thickness based bunching strategy utilized for the measuring a limit work for the preparing and identification of DOS assault. In the proposed system, DOS ambush distinguishing proof is done in two phases. In the preliminary time of revelation process, RTT and hop number is used to recognize the proximity of DOS attack. Since veritable division secured is more, RTT of the course with DOS ambush will be high when differentiated and a common course having a comparable number of bobs [11-13]. Inside seeing a DOS ambush, the packs travel more detachment along the DOS associate, for all intents and purposes equal to 8 or 9 hops, which won't be incorporated the skip count of RREP send by the attackers. This perceives a normal course from a DOS interface. Once a course is suspected, proposed gathering computation is done to confirm the proximity of DOS strike and to limit the aggressors. While batching, every center point along the course transforms into the Cluster Head (CH) and packs the centers into different gatherings. In the wake of packing, the source center point will confirm the closeness of DOS attack by sending an exceptional control message-Cluster Request (CREQ) to the accompanying center along the course, if that center point is a gathering part. So additionally, this CREQ will be sent by coming about centers along the course until, the accompanying center point is no longer bundle part or when objective is come to the modified protocol is called multiple constraints on demand routing protocol (CHAODV)[25][26]. The CHAODV protocol based on two functions one is threshold based function and one is MBC function. The threshold based function measure the distance of mobility of node during the process of communication [10]. The mobility of node measure in two different scenarios. In 1st scenario measure the same level of path and 2nd level used in case of different path [15-17]. For the evaluation of performance our modified protocol tested in different network scenario tested through simulations for different distributions of nodes in different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent routing probabilities with few path failures that depend on the value of threshold. The rest of paper discuss as section II. Clustering technique in section III discuss the improved Algorithm of AODV. In section IV discuss the Experimental result analysis and finally discuss conclusion & future work.

II. Clustering Technique

Thickness based bunching techniques aggregate neighbouring articles into groups in light of nearby thickness conditions as opposed to closeness between items [1]. These techniques see groups as thick areas being isolated by low thickness uproarious locales. Density–based strategies have clamour resilience, and can find non-arched groups. Like various leveled and parcelling strategies, thickness based systems experience troubles in high dimensional spaces in view of the natural shortage of the component space, which thus, lessens any grouping inclination. Thickness based Spatial Clustering of Applications with Noise (DBSCAN) looks for center questions whose area (span) contains at any rate Minpts focuses[27]. An arrangement of centre articles with covering neighborhoods characterize the skeleton of a group. Non-centre focuses lying inside the area of centre items speak to the limits of the bunches, while the remaining is clamor. DBSCAN can find self-assertive formed groups, is inhumane to anomalies and request of information info, while its multifaceted nature is O (N2). In the event that a spatial file information structure is utilized the intricacy can be enhanced up to O (N log N) [7]. DBSCAN separates in high dimensional spaces and is exceptionally touchy to the information parameters and Minpts [26].

III. Proposed Algorithm

In this section discuss the improved protocol of AODV protocol. The modified AODV protocol used threshold function for the detection of DOS node. The threshold function used density based clustering technique based on hop count and round-trip time.

Steps of algorithm

1: define the value of region $R_1, R2, R3, \ldots., R_n,$; according to their region of vehicles
2: For any node velocity Vi $\in$ R proceed
3: v_i forms a list of its region node R(i) send the control messages {STR_CC};
4: $N(i) = \varphi$;
5: estimate the value of threshold TH_i :
6: $TH_i = Xri + vi * \text{total send packet} + Rtt$;
7: define set value of vehicles nodesvi $\in$ R
8: $RH = 0, \text{traffic} = 0;$
9: node = "None";
10: Repeat
11: Any node $v_i \in$ Rsend control message
12: If R(i) $<> \varphi\ Then$
13: select v $\in$ N(i) ;
15: Else vi is a CR of itself.
EndIf
16: Update the region of traffic CR;
17: CR = ID;
18: traffic = 1;
19: Node = malicious;
20: $J = \text{Count}(N\ [RTT])$;
22: For $I = 1$ to J Do
23: If ($n_i \in N$ [CR] receives the message &&$v_i \rightarrow CR = 0$)
24: Then V_i sends a message "RTT_CC" to CR
25: If ($CR \rightarrow RTT < THi$)
26: Then CR sends a message "normal node ;
27: CRproceed for next region;
28: $CR \rightarrow \text{traffic} = CR \rightarrow \text{Traffic} - 1;$
29: v_i proceed for next threshold;
30: $vi \rightarrow CR = CR \rightarrow RTT\_CC$
31: Else go to 10;
EndIf
EndIf
End For
32: UPDATE ($Cr \rightarrow \text{traffic} = THi$);
End.

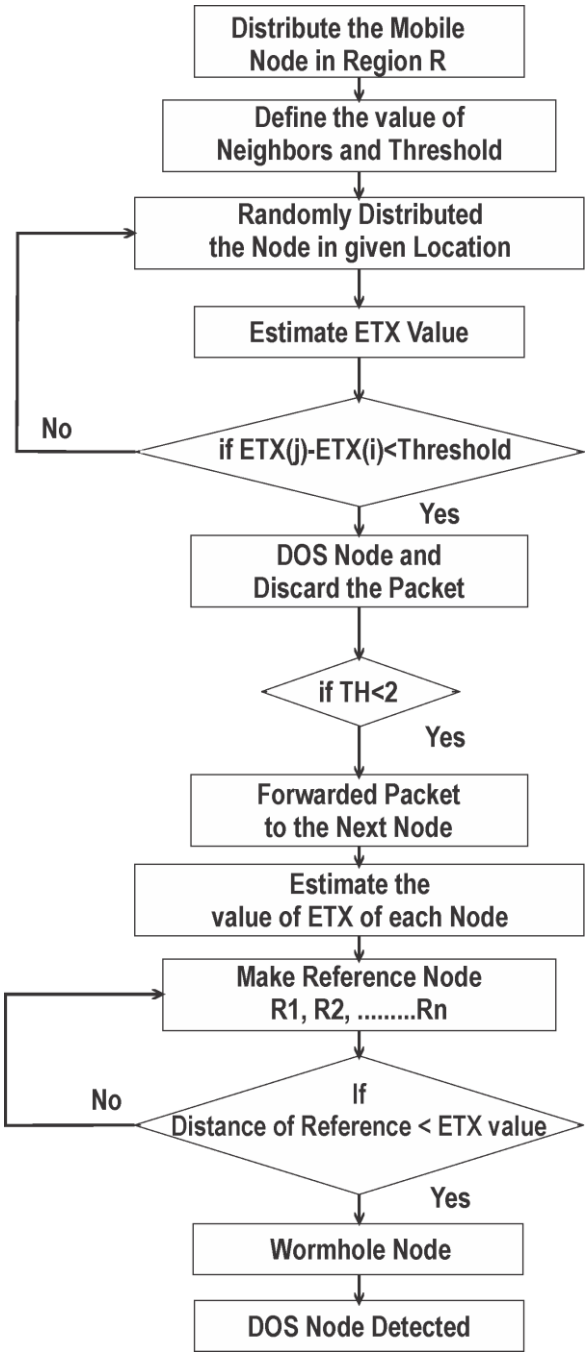

Figure 1: proposed model of DOS attack detection in VANET network based on cluster threshold function.

IV. Simulation & Result Analysis

Simulation is an experimental process in that process proposed a simulated model for VANET network and put some standard parameter for valuation of result. In our research work perform rural area traffic in VANET network. The proposed model of CHAODV written in MATLAB language and scenario of network generated by SUMO software as input of protocol. Different performance metrics are used to check the performance of proposed model in various network environments. In our experiment, we have selected throughput and packet drop to check the performance of VANET proposed model protocols against denial of service attack. The reason for the selection of these performance metrics is to check the performance of proposed model protocols in highly mobile environment of VANET. Moreover, these performance metrics are used to check the effectiveness of VANET proposed model protocols i.e. how well the protocol delivers packets and how well the algorithm for a proposed model protocol performs in order to discover the route towards destination. The selected metrics for proposed model protocols evaluation are as follows:

Performance Parameter

- **Throughput:** Throughput provides the fraction of the data rate used for helpful transmission and is outlined because the total range of packets received by the destination [14][15]. it's in truth a live of the effectiveness of a routing protocol [16].

A network outturn is that the average rate at that message is with success delivered between a destination node (receiver) and supply node (sender). it's conjointly remarked because the quantitative relation of the number of information received from its sender to the time the last packet reaches its destination. Outturn may be measured as bits per second (bps), packets per second or packet per interval. For a network, it's needed that the outturn is at high-level [12]. Some factors that have an effect on MANET's outturn square measure unreliable communication, changes in topology and information measure.[10] merely the entire knowledge transmitted per second is named outturn of network

- **Average End-To-End Delay:** This includes all doable delays caused by buffering throughout route discovery latency [7], [8] queuing at the interface queue, retransmission delays at the macintosh, and propagation and transfer times [9].

This is the common time concerned in delivery of knowledge packets from the supply node to the destination node [22]. To calculate the common end-to-end delay, add each delay for every flourishing knowledge packet delivery and divide that add by the quantity of with success received knowledge packets. [23].

- **Packet Delivery Ratio:** The magnitude relation of the info packets delivered [9] to the destinations to those generated by the traffic sources.

The packet delivery magnitude relations are often calculated by dividing range of packets received by range of packet sent [12]. This performance metric provides North American country a thought of however well the protocol is playacting in terms of packet delivery at totally speeds victimization different traffic models [17].

MATHEMATICALLY EXPRESSION [18-21]

Average PDR (%)

$$\text{PDR} = \sum_{i=1}^{m} \frac{\text{by each destinationdata packets received Addition}}{\text{m}}$$

Where,

i, symbol of the number of output file
m, symbol of the total number of output files

Normalized Routing Load

$$\text{Normalized Routing Load} = \frac{\text{Total Routing Packets Sent}}{\text{Total Data Packets Received}}$$

Average End to End Delay

$$\text{Average End to End Delay} = \frac{\sum \text{Total Data Packets Received}}{(\text{Time Received} - \text{Time Sent})}$$

PACKET DELIVERY RATIO

AODV	0.63	0.82	0.56	0.55	0.42	0.37
CTAODV	0.55	0.67	0.51	0.48	0.3	0.32

Table 1: present those comparative values of PDR with AODV and CTAODV method.

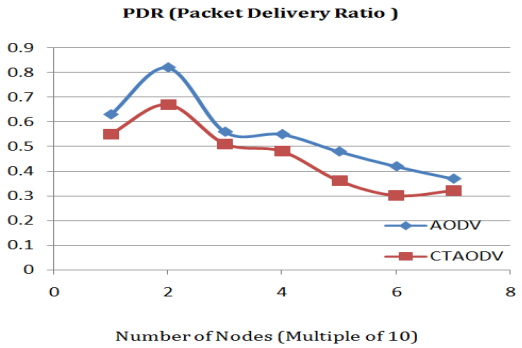

Figure 2: PDR vs. Number of nodes.

Packet Delivery Ratio result value of both method AODV and CTAODV, here CTAODV show better performance compare to AODV.

NORMALIZED ROUTING LOAD

It is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received [20]. It can be observed that AODV has more routing overhead compared to both the CT AODV.

AODV	58005	88005	20005	55005	60005
CTAODV	65005	99505	21005	79005	74005

Table 2: Present those comparative values of routing Overhead with AODV and CTAODV method.

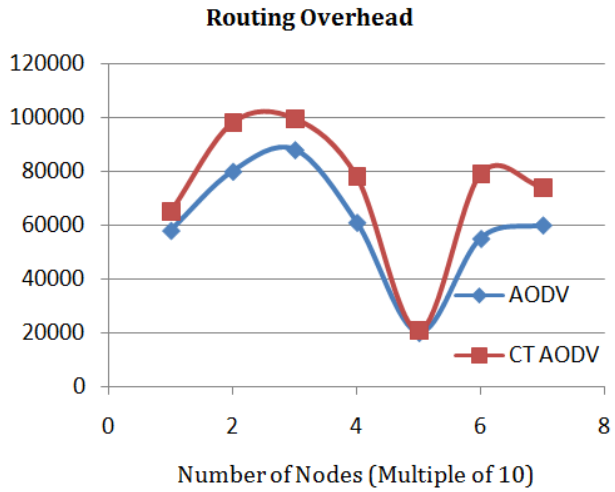

Figure 3: Normalized Routing Load Vs Number of Nodes.

.Routing Overhead result value of both method AODV and CTAODV, here CTAODV show better performance compare to AODV.

AVERAGE END TO END DELAY

We can observe that AODV achieves reduction in average end to end delay. This can happen because AODV has the minimum hop route and CTAODV has a route with higher no of hops than AODV.

AODV	15550	20050	17050	18050	22050
CTAODV	22050	22550	20050	21050	24050

Table 3: present that comparative values of End_to_End Delay with AODV and CTAODV method.

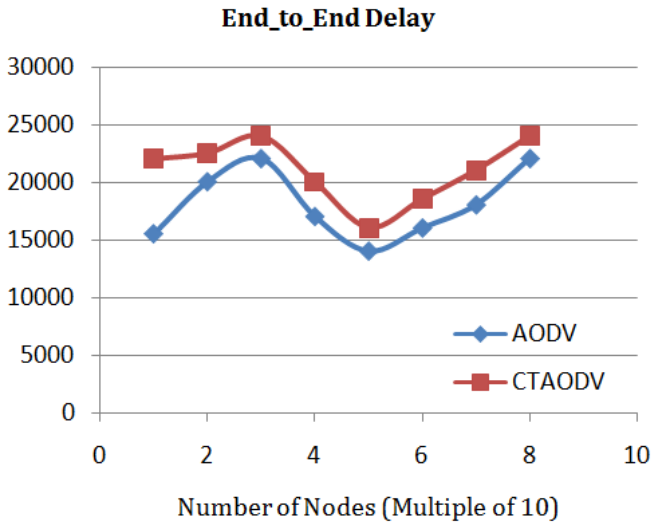

Figure 4: Average End to End Delay Vs Number of nodes.

End_to_End Delay result value of both method AODV and CTAODV, here CTAODV show better performance compare to AODV.

THROUGHPUT

AODV has a better end to end delay which will help to improve the throughput of the network. Reduced throughput of CTAODV compared to AODV suggests that throughput is a trade-off to achieve stable route.

AODV	325	415	315	295	355
CTAODV	375	485	395	355	405

Table 4: present that comparative values of Throughput with AODV and CTAODV method.

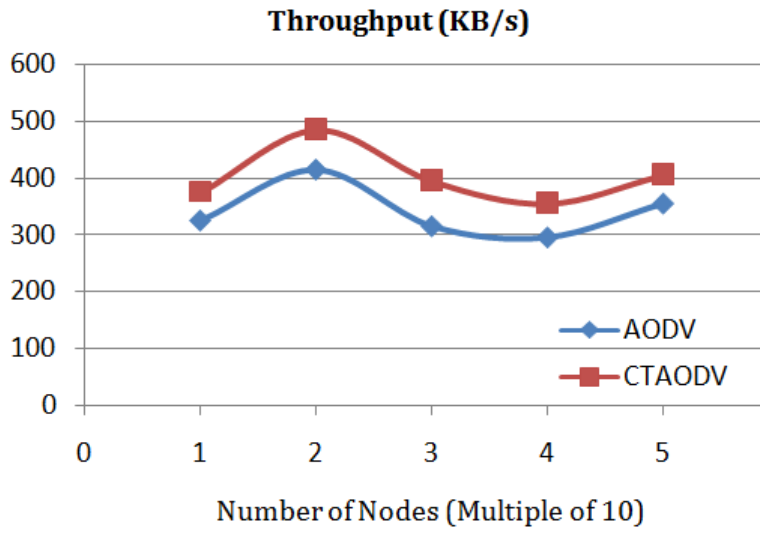

Figure 5: Throughput Vs Number of Nodes**.**

Throughput result value of both method AODV and CTAODV, here CTAODV show better performance compare to AODV.

V. Conclusion & Future Scope

DOS identification and avoidance is real test in VANET network. The excellence of DOS assault, the discovery procedure is extremely troublesome. In this paper adjusted the AODV convention with group based method. The group based procedure utilized the edge work for the discovery of DOS detection. As to DOS come about, gives an efficient computation to neighbor disclosure and DOS shirking. It thoroughly addresses diverse convenient obstructions of the earlier procedures. The power used to actualize the new approach is less when contrasted with the before work. The neighbor revelation calculations will diminish the crash happen amid information transmission and course every parcel accurately to the goal recipient. This work has concentrated on identifying the DOS not to evacuate that DOS. Future work incorporates building up a strategy for expulsion of the DOS when it identified with the assistance of this proposed approach. In this work it is by all accounts that system parcel has expanded. Because of number of parcels the execution of system can decreases. It likewise expands the system conjunction. So there is have to decrease the parcels in the system. It has been likewise watched that there are different extensions to enhance the proposed strategy.

References

[1]. Congyi Liu, ChunxiaoChigan and Chunming Gao "Compressive Sensing based Data Collection in VANETs", IEEE, 2013, Pp 1756-1761.
[2]. Narendra Mohan Mittal and Savita Choudhary "Comparative Study of Simulators for Vehicular Ad-hoc Networks (VANETs)", International Journal of Emerging Technology and Advanced Engineering, 2014, Pp 528-537.
[3]. Duc Ngoc Minh Dang, Choong Seon Hong, Sungwon Lee and Eui-Nam "An Efficient and Reliable MAC in VANETs", IEEE, 2014, Pp 616-619.
[4]. Mahmoud Hashem Eiza and Qiang Ni "An Evolving Graph-Based Reliable Routing Scheme for VANETs", IEEE, 2013, Pp 1493-1504.
[5]. Ming-Chin Chuang and Meng Chang Chen "DEEP: Density-Aware Emergency Message Extension Protocol for VANETs", IEEE, 2013, Pp 4983-4993.
[6]. N. Sakthipriya and P. Sathyanarayanan "A Reliable Communication Scheme for VANET Communication Environments", Indian Journal of Science and Technology, 2014, Pp 31-36.

[7]. Ramon Bauza, Javier Gozalvez and Miguel Sepulcre "Power-Aware Link Quality Estimation for Vehicular Communication Networks", IEEE, 2013, Pp 649-652.
[8]. Alejandro Cornejo, SairaViqar and Jennifer L. Welch "Reliable Neighbor Discovery for Mobile Ad Hoc Networks", ACM, 2010, Pp 1-10.
[9]. Khalid Abdel Hafeez, Lian Zhao, Bobby Ma and Jon W. Mark "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications", IEEE, 2013, Pp 3069-3083.
[10]. Mohamed Ahmed, Mohammad Reza JabbarpourSattari, Mostofa Kamal Nasir, SaeidGhahremani, SajadKhorsandroo, Syed Adeel Shah Ali and Rafidah Md Noor "Vehicle Adhoc Sensor Network Framework to Provide Green Communication for Urban Operation Rescue", GREEN COMMUNICATIONS, 2013, Pp 77-82.
[11]. Karan Verma, HalabiHasbullah and Ashok Kumar "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", IEEE, 2012, Pp 550-555.
[12]. Jacek Rak "Providing Differentiated Levels of Service Availability in VANET Communications", IEEE, 2013, Pp 1-4.
[13]. Marica Amadeo, Claudia Campolo and Antonella Molinaro "Design and Analysis of a Transport-Level Solution for Content-Centric VANETs", IEEE, 2013, Pp 1-6.
[14]. Ivan Stojmenovic "Machine-to-Machine Communications with In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems", IEEE, 2014, Pp 122-128.
[15]. Celimuge Wu Satoshi Ohzahata and Toshihiko Kato "Flexible, Portable, and Practicable Solution for Routing in VANETs: A Fuzzy Constraint Q-Learning Approach", IEEE, 2013, Pp 4251-4263.
[16]. Duc Ngoc Minh Dang, Hanh Ngoc Dang, VanDung Nguyen, ZawHtike and Choong Seon Hong "HER-MAC: A Hybrid Efficient and Reliable MAC for Vehicular Ad hoc Networks", IEEE, 2014, Pp 186-195.
[17]. Xiaomin Ma, Xiaoyan Yin, Matthew Wilson and Kishor S. Trivedi "MAC and Application-Level Broadcast Reliability in VANETs with Channel Fading", IEEE, 2013, Pp 756-761.
[18]. M. Milton Joe, Dr. B. Ramakrishnan and Dr. R. S. Shaji "Modeling GSM Based Network Communication in Vehicular Network", MECS, 2014, Pp 37-43.
[19]. Rasheed Hussain and Heekuck Oh "Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks", JIPS, 2014, Pp 103-118.
[20]. Ian Ku, You Lu, Mario Gerla, Francesco Ongaro, Rafael L. Gomes and Eduardo Cerqueira "Towards Software-Defined VANET: Architecture and Services", IEEE, 2014, Pp 1-8.
[21]. Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre and Alejandro Quintero "VANET security surveys", Elsevier, 2014, Pp 1-13.
[22]. EghbalHeidari, Alexander Gladisch, Behzad Moshiri and DjamshidTavangarian "Survey on location information services for Vehicular Communication Networks", springer, 2013, Pp 1-22.
[23]. Omar Abdel Wahab, HadiOtrok and Azzam Mourad "VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks", Computer Communications, 2013, Pp 1422–1435.
[24]. AngelosAntonopoulosa, CharalabosSkianisb and Christos Verikoukis "Network Coding-based Cooperative ARQ Scheme for VANETs", Journal of Network and Computer Applications, 2011, Pp 1-28.
[25]. Sudipto Guha, Nina Mishra, Rajeev Motwani and Liadan O'Callaghan "Clustering Data Streams", Springer, 2016, Pp 1-8.
[26]. Qinbao Song, Jingjie Ni and Guangtao Wang "A Fast Clustering-Based Feature Subset Selection Algorithm for High Dimensional Data", IEEE, 2013, Pp 2-16.
[27]. A. Sancho-Asensio, J. Navarroa, I. Arrieta-Salinas, J. E. Armendáriz-Ínigo, V. Jiménez-Ruanoa and A. Zaballosa, E. Golobardes "Improving Data Partition Schemes in Smart Grids Via Clustering Data Streams", ACM, 2015, Pp 23-44.

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Nidhi Saxena. "Enhanced the Performance of VANET Network Using Clustering Based Thresholding Technique for Reliable Communication." IOSR Journal of Computer Engineering (IOSR-JCE) 21.2 (2019): 32-38.