FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Research Article | Volume 2, Issue 2 | Pages 31-35 | ISSN XXXX-XXXX

Meta-heuristic VOIP Stream Aggregation with Abnormality Aware Traffic Inflow Evaluation

Lovepreet Kaur[1], Rajdeep Kaur[2] and Prabhjot Kaur[2]

[1]*Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India, luvprit11@gmail.com*
[2]*Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India, rajdeep.cu85@gmail.com*
[3]*Department of Computer Science & Engineering, Chandigarh University, Gharuan, Punjab, India, mannprabh17@gmail.com*

***Correspondence:** *luvprit11@gmail.com*

ABSTRACT- The voice over IP models are growing rapidly as they cost far less than the traditional voice phone networks. The VOIP network utilizes the internet service-based IP network for the transfer of the voice data between the two destinations, which connects the various companies across the globe with far less expense. In this paper, the major focus has been kept at the aggregation of the voice data over the major controller switches in the IP network. The aggregation module utilizes the meta-heuristic voice streams for the preparation of the single aggregated stream. Also, the proposed model aims at the security level of the aggregation by minimizing the abnormalities tracked by using the concept of the higher and lower thresholds, which empowers the proposed model for the secure propagation of the voice data. The experimental results show the higher accuracy and significance of the proposed model in the terms of aggregation model and higher security.

Keywords: Abnormality Detection, Floating Threshold, Reporting Interval, VoIP aggregation.

ARTICLE INFORMATION

Author(s): Lovepreet Kaur, Rajdeep Kaur and Prabhjot Kaur;
Received: 11/04/2023; **Accepted**: 19/06/2023; **Published**: 30/06/2023;
e-ISSN: XXXX-XXXX;
Paper Id: IJCSR-020201;
Citation: 10.37391/IJCSR.020201

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Wireless mesh network (WMN) is a network made up of radio nodes which are organized in mesh topology. It is the extension of adhoc and wireless sensor networks. WMN has self-organized and self-configured nature. It consists of mesh routers, mesh clients and gateways. Mesh clients are end users like laptops, these devices have limited power, they may or may not be connected to network. WMN routers route the network traffic but they cannot originate or terminate the traffic. WMN gateways are routers with direct access to network. To improve the flexibility of mesh network, a mesh router furnished with multiple wireless interfaces. Compared with conventional routers, a mesh router can achieve same coverage with low transmission power through multi-hop communication. Wireless Mesh Network consists of wireless networks connected by a wireless backbone. They are easily deployed and have low cost overhead as compared to optical networks. It has self-optimizing, fault-tolerant and self-organizing nature.

A mesh network is reliable because if any node stops working then other nodes communicate with each other directly or with the help of interfaces. WMN is fully wireless network that uses multi-hop communication technique to communicate over the network.

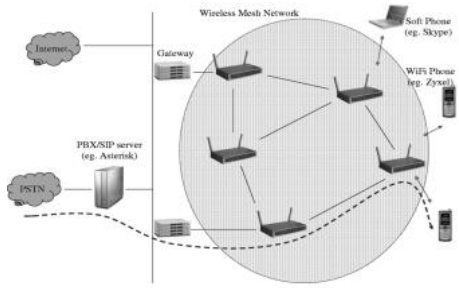

Figure 1: Path Maintenance in mesh network between two clients [16]

VoIP is an emerging technology used to transmit voice communication over internet protocol. VoIP (Voice over IP) deliver multimedia sessions and voice communication over internet protocol. Others names for VoIP are broadband telephony, internet telephony, broadband phone service and IP telephony. VoIP uses public internet instead of public switched telephone network (PSTN). VoIP calls are similar to traditional telephone. Instead of transmitting voice signals over circuit switched network, it packetized data and transmit these packets over packet switched network. A VoIP service deployment scenario over wireless mesh network is shown in figure 1.1. In this scenario VoIP service has ability of accessing the fixed or wired phones to wireless VoIP phones. The popularity of VoIP services increases these days. To fulfil the consumer demands for VoIP services regardless of their location needs broad area coverage. For improving the VoIP services performance, packet aggregation techniques are done. Packet aggregation means aggregating multiple packets to form a single large packet. Aggregation done at different layers like Network, MAC and Application layer. Aggregation at Network layer done by aggregating IP packets and called as packet aggregation. Aggregation at MAC layer done by aggregating frames and

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Research Article | Volume 2, Issue 2 | Pages 31-35 | ISSN XXXX-XXXX

called as frame aggregation. Aggregation at application layer done by aggregating audio frames. In packet aggregation, instead of sending multiple small packets with separate headers, it aggregate those small packets and send them with single header. It does not reduce only overhead but also saves time.
During aggregation, packets which need to be combined should be in queue. And queuing is attained using force delay aggregation. Packets are assigned a time stamp in force delay aggregation and each packet is allotted a maximum delay time. When this delay time expired, a node will start to combine packets which are going towards the same destination. According to force delay aggregation method, the maximum number of packets to be combined is administered by maximum transmission unit. For wired, MTU is 1500 bytes and for wireless networks, it is 23000 bytes. VOIP (Voice Over Internet Protocol) traffic is reactive to delay, for this reason the packet which is not able to aggregate within maximum delay time, is transmitted immediately un-aggregated. Hence, it is crucial to select the correct maximum delay time. Aggregation is of two types: Hop-to-hop aggregation and end-to-end aggregation.

Hop-to-hop aggregation: In hop-to-hop aggregation, aggregation and de-aggregation done at every hop until the packet reached at its destination. This process cause higher delay.

End-to-end aggregation: In end-to-end aggregation, aggregation is done only at transmitting node and de-aggregation is done at receiving node. This type of aggregation is suitable for packets that are going toward common destination and intermediate nodes are just responsible for packet advancement. Hence, end-to-end delay is less.

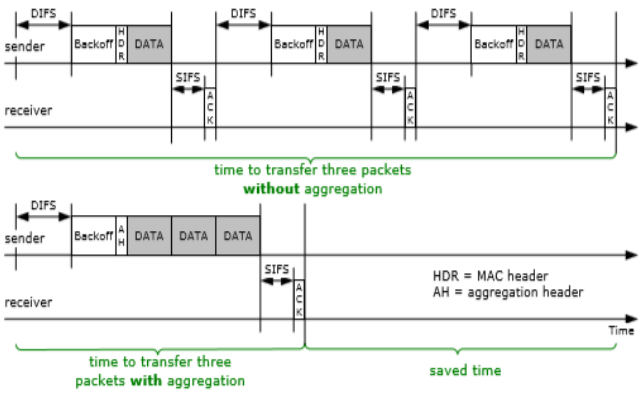

Figure 2: Packet Aggregation of three nodes [10]

1.1 Security Issues

Internet is basically a platform where each and every one can send and receive packets and also demands some mechanisms for securing communication on it. In Public Switched Network, eavesdropping can be difficult but it is easier in IP networks. Audio streams, video streams etc. all need some type of protection. In real time communications, security is essential by ensuring authentication of calls which prevents some type of attacks like DOS (Denial of Service) attack, eavesdropping, injection attack etc. Security in VoIP consists of securing the call initialization, its management and also include protection of bills. VoIP calls are also charged by the billing mechanism which should be perfectly secured and implemented.

2. RELATED WORK

Muhammad Shahzad Asif et.al.[1] proposed a decision-oriented model named AADM (Adaptive Aggregation based Decision Model). On the basis of link quality, AADM take decision about the type of aggregation should be used to achieve desired results. In AADM, aggregation is done on the basis of various parameters such that BER (Bit Error Rate), PLR (Packet Loss Ratio), congestion, bandwidth, buffer size, energy consumption and delay. It dynamically takes decisions whether the aggregation is required or not. It also defined MTU (Maximum Transmission Unit) for aggregation. It finally decides the type of aggregation i.e. hop-to-hop aggregation or end-to-end aggregation is suitable for the data. Then, it decides that whether system aggregate both non real time and real time data according to bandwidth, otherwise it consider only real time traffic. AADM also specify the role of sender and receiver in the aggregation mechanism. Jyoti Rajput et.al. [3] discussed about WSN (Wireless Sensor Network), data aggregation and its various approaches, security issues in data aggregation and comparison of various security protocols. Data aggregation is done with the help of functions such as COUNT, AVG, SUM, MIN, MAX etc. Data aggregation approaches used in this paper are centralized approach, network aggregation approach and decentralized approach. This paper discussed about the security facts that are required in data aggregation i.e. confidentiality of data, freshness of data, integrity of data and source authentication. It also discussed about the attacks on data aggregation and various security protocols i.e. secure information aggregation (SIA), secure hop-by-hop data aggregation protocol (SDAP), synopsis diffusion for robust aggregation in sensor networks, reputation based secure data aggregation (RSDA).

Giovanni Di Stasi et.al.[4] proposed a technique called aggregation aware forwarding which overcome the limitation that packet aggregation and multipath routing are not work well together. It allows multipath routing and packet aggregation simultaneously to increase the network performance. This technique does not alter the path computation module but changes the sense of forwarding decisions. This method of combining the multipath routing and packet aggregation reduces end-to-end delay and increases throughput. Mantao Wang et.al.[5] presented an reliable and energy efficient aggregation for wireless sensor networks. In this paper a reputation based data aggregation method is proposed for wireless sensor network, in which aggregator or cluster head is selected on the basis of its reputation value and its residual energy, so that the nodes with high reputation and residual energy will be selected. In the end energy efficiency and reliability can be obtained. Khyati Marwah et.al.[6] focused on evaluating the consequences of packet aggregation on different parameters like end-to-end delay, Mean Opinion Score (MOS) and aggregation delay. This paper investigated the VOIP (Voice Over Internet Protocol) performance over Wireless Mesh Network and resolved the various challenges faced by VOIP.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Computer Science Research (IJCSR)
Research Article | Volume 2, Issue 2 | Pages 31-35 | ISSN XXXX-XXXX

VOIP packets are tiny in size and small size packets cause high overhead because they use different headers. Due to which a large amount of bandwidth is wasted on it. To overcome the above problem, this paper does packet aggregation. Ian F.Akyildiz[17] presented a survey on wireless mesh network. In which network architecture and design factors of wireless mesh network was discussed. The architecture of wireless mesh network categorised in three categories: infrastructure or backbone WMNs, client WMNs and hybrid WMNs. The design factors which affect the performance of WMNs are: scalability, radio techniques, broadband and QoS, mesh connectivity and compatibility.

3. ANOMALY DETECTION & FILTERING ALGORITHM (ADFA)

Data filtering or data overhead filtering is used to filter the data coming from unknown or known nodes. The aim of proposed model is to protect against injection attack. The proposed model is designed to detect the very low or very high traffic turnout coming from different sources in order to detect the anomaly which is not permitted according to rule of receiving the traffic. According to the requirement traffic rules are updated with continuous scanning being performed over the nodes. The algorithm in proposed model calculates the dynamic threshold for the purpose of detection of the attack and for the filtering of attack traffic. The, proposed model is designed to calculate the threat cause by arrack from unauthorized or authorized sources. The proposed model design has been given below:

Algorithm 1: Attack Traffic Mitigation Algorithm

1. Available bandwidth on the node is calculated by anomaly detector (Ax).
2. Ax scan active connections of the analyzed node.
3. Ax analyse input data volume D= {dv1, dv2, dv3 … dvX} coming from various nodes.
4. Ax compute the D matrix and decide the threshold value.
5. Individual data volume scanned against the threshold value (Th) to find the traffic abnormalies.
6. Abnormal traffic noticed from traffic strearm volumes and analyzed individually.
7. Traffic volume is calculated and compare with the assigned individual connection bandwidth.
8. If the traffic volume is found more than Connection Bandwidth,

   The overhead traffic is filtered.

   Otherwise

   The traffic is filtered.

The dynamic rule updation algorithm is based on the anomaly detector (Ax) and traffic flow analyzer furnished with dynamic traffic flow control mechanism. The traffic irregularity scanning method is deployed over the live traffic being received from different sources over the central switch has been considered for the dynamic flow control methodology. The voice over IP (VOIP) traffic generated by the nodes is dynamically aggregated in order to increase the throughput and reduce the latency across the end-to-end communication paths. The following algorithm has been decided for the realization of the proposed VOIP data aggregation model.

Algorithm 2: Dynamic Rule updation algorithm

1. When the VOIP input stream count becomes more than one for the similar subnet over the existing connection between two switches.
   a. The aggregation procedure begins.
   b. Aggregate id is created (Ag).
2. For each aggregate $\partial \in D$ perform the following:
   a. Add ∂ to the aggregate stream list with all properties.
   b. Update the aggregate transmission time to 0.
   c. Start the life timer for the lifetime tracking of aggregate.
3. While performing the anomaly detection algorithm over input streams.
   a. For set of packets or every packet in the input stream.
      i. Calculate the maximum and minimum traffic volume limits.
      ii. If current data Limit is lower than the lower limit, then expand the aggregate and add the new stream to the aggregate stream.
      iii. Otherwise if current data limit under the higher limit, then contract the aggregate stream and do not add the new data stream to the aggregate stream.
   b. If $\sum \partial$ smaller than the permitted limit A, then
      i. If current data limit is lesser than the lower limit, then expand the aggregate and add the new stream to the aggregate.
      ii. Otherwise if current data limit will be under the higher limit, then contract the aggregate stream and do not add the new stream data to the aggregate.

Algorithm 3: Rule Placement Algorithm

1. For every data input stream in the aggregate
   a. Collect the data from all open switch ports denoted with $\sum \partial$.
   b. If the data is under the available output limit
      i. Increase the individual flow covering count or flow share for each entry in the aggregate.
      ii. Assign current traffic volume as the standard traffic volume.
   c. If traffic flow ends
      i. Use the $\prod_{i=1}^{N} \partial$ equation to remove the selected flow id from the active traffic.
      ii. Remove the candidate id of the origination node

4. RESULT ANALYSIS

The proposed model has been designed for the purpose of the security of VOIP model over the IP network. The proposed model has been designed in the four-zonal topological model, which has been shown in the *figure 3*.

FOREX Publication
Open Access | Rapid and quality publishing

International Journal of Computer Science Research (IJCSR)
Research Article | Volume 2, Issue 2 | Pages 31-35 | ISSN XXXX-XXXX

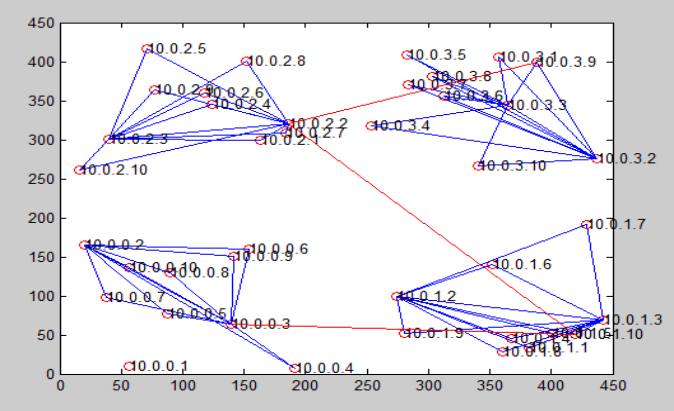

Figure 3: Topological model of VOIP security over IP network

The *figure 3* shows the four IP subnets, which can be defined as the separate zones and has been divided by the subnet division. The subnet mask of 255.255.255.0 (24) has been utilized for the testing of the proposed model. The 10.0.0.0/8 has been selected as the base network and first four subnets divided by the 24-bits subnet mask has been utilized for the purpose of the zonal division of the IP network. In the data aggregates, the major issues lie with the level of security, which arises with the receiving of the anomalies. The anomalies must be detected and avoided in the minimum possible time, which is known as the detection delay or the delay in detection. The following figure (*Figure 4*) describes the results obtained for the detection delay of the abnormalities in the aggregate data. The ingress data is actively scanned against the permitted threshold limits, which holds the key to analyze and detect the anomalies in the VOIP traffic inflow over the switching units.

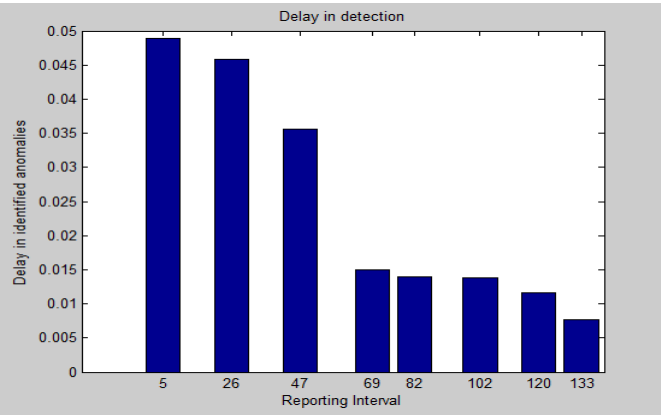

Figure 4: The delay in detection in the aggregation data

The *figure 4* describes the delay in detection of the anomalies on the different reporting intervals. The variable reporting intervals have been taken into account for the evaluation of the anomaly detection. The results of the anomaly detection have shown the decrease the anomaly count as the simulation network convergence level increases.

5. CONCLUSION

The model has been proposed for the voice of IP (VOIP) networks along with the protection of the VOIP networks from the anomalies. The proposed model has been designed for the purpose of VOIP data aggregation, which can hold the multiple streams altogether under the one aggregated stream inflowing between the two primary network switches handle the voice data. The aggregated data is always prone to the malicious code injections, which is largely demonstrated by the extremely high or low traffic inflows, which dwarfs the chances of detection. The proposed model has been designed by keeping this into the account. The proposed model has been evaluated for the anomaly count in the VOIP data inflow. The anomaly detection method is based upon the bottom and higher threshold limits, which increases the integrity of the aggregation under the proposed VOIP data aggregation model. The experimental results have justified the claim of the security by admitting the abnormalities in the traffic inflows over the different reporting intervals.

REFERENCES

[1] M.S.Asif , M.Shafiq. J.G. Choi, M.Iqbal, A.Irshad, “Flexible and efficient aggregation framework for antifragile wireless mesh networks”, International Journal of Reliable Intell Environ, Springer International Publishing, pp.159-171, 2015.

[2] Adyasha Behera and Amrutanshu Panigrahi, “Determining the network throughput and flow rate using GSR and AAL2R”, International Journal of UbiComp(IJU), vol.6,no.3.pp.9-18,2015.

[3] Jyoti Rajput and Naveen garg, “A survey on Secure Data Aggregation in Wireless Sensor Network”, International Journal of Advanced Research in Computer Science and Software Engineering, vol.4, issue.4,pp.407-412,2014.

[4] G.D.Stasi, J.Karlsson, R.Canonico, A.Brunstrom, "Combining multi path forwarding and packet aggregration for improved network performance in wireless mesh networks", Computer Networks, Elseveir B.V.,pp.26-37,2014

[5] M. Wang,J. Wei,Y. Pan,Z. Zhao,"Study on Reputation and Trust Based Data Aggregation Schemes for Wireless Sensor Networks", IEEE 7th International Conference on Advanced Infocomm Technology, pp.79-84,2014.

[6] Khayati Marwah and Gurpal Singh, “VOIP over WMN:Effect of packet Aggregation”, International Journal on Computer Science and Engineering,vol.3,no.6,pp.2323-2331,2011.

[7] Kun-chan Lan and Tsung-hsun Wu, “Evaluating the perceived quality of Infrastructure-less VoIP”, IEEE International Conference on Multimedia and Expo, pp.1-6, 2011.

[8] R. K. Kehal and Dr.J. Sengupta, “A comprehensive Review on Improving QOS for VOIP in Wireless Mesh Networks”, Journal of Global Research in Computer Science, vol.2, no.8, pp.32-33, 2011.

[9] M.K.Jha and T.P Shrama, “A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks”, International Journal on Computer Science and Engineering, vol. 2, no.5, pp.1539-1543, 2010.

[10]]P.Dely, A.Kassler, N.Bayer, H.J. Einsiedler, D.Sivchenko, “FUZPAG: A Fuzzy-Controlled Packet Aggregation Scheme for Wireless Mesh Networks”,IEEE 7th International Conference on Fuzzy Systems and Knowledge Discovery, pp.778-782, 2010.

[11] Yi Ping, X. Hongkai, Wu Yue, Li Jianhua1, “Security in Wireless Mesh networks:Challenges and Solutions”, IEEE 6th International conference on Information Technology:New Generations, pp.423-428, 2009.

[12] Hani Alzaid,Ernest Foo and Juan Gonzalez Nieto, “Secure Data Aggregation in Wireless Sensor Network: A Survey”, Australian Information Security Conference ,2007.

[13] R. Baumann, S. Heimlicher, V. Lenders, M. May, “Routing Packets into Wireless Mesh networks”, IEEE 3rd International Conference on Wireless and Mobile Computing, Networking and Communications, 2007.

International Journal of
Computer Science Research (IJCSR)
Research Article | Volume 2, Issue 2 | Pages 31-35 | ISSN XXXX-XXXX

[14] D. Niculescu, S. Ganguly, K. Kim, R.Izmailov, "Performance of VoIP in a 802.11 Wireless Mesh Network", in the Proceedings of IEEE INFOCOM,pp.1-11,2006.

[15] S. Waharte, R. Boutaba "Routing protocols in wireless mesh networks: challenges and design considerations", Multimedia Tools and Applications, vol 29, pp. 285-303, 2006.

[16] S. Ganguly, V. Navda,K.Kim, A. Kashyap, D. Niculescu, "Performance Optimizations for deploying VOIP services in Mesh Networks", IEEE Journal on Selected Areas in Communications, vol.24,no.11, pp.2147-2158, 2006.

[17] Ian F. Akyildiz and Xudong Wang, "A survey on Wireless Mesh Networks", IEEE Radio Communications, pp.S24-S30, 2005.

[18] Marko Leppänen, "Voice over IP", Seminar on Internetworking, pp.1-12, 2001.