System Performance of Adaptive Bandwidth Traffic Shaping Mechanism for Residential Safety System

Putri S. Khalid and Wahidah Hashim
MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
Email: {shahnim.khalid; wahidah.hashim}@mimos.my

***Abstract*—A study on system performance of an adaptive traffic shaping mechanism for residential safety system is proposed and discussed in this paper. Traffic shaping is a way to help increase network performance by controlling the amount of data that flows into and out of the network. With new types of applications, traditional traffic shaping techniques may not be sufficient to solve problems in more dynamic clients' applications. In order to solve the problem efficiently, we present an adaptive traffic shaping for distributed clients connected to the residential safety system which is enabled depending on client's request made to the server, hence priority access is given. This method does improve the quality of service in the network as shown in both of our simulation and real data results by reducing almost 99% rate of discarded data in the network. In addition, the corresponding performance is further compared between audio and video data in order to see percentage of data lost when employing our adaptive traffic shaping mechanism. Finally, both distributed clients are compared in terms of data transferred whenever the mechanism is enabled. Simulations results obtained indicate the proposed algorithm is effective and feasible.**

***Index Terms*—traffic shaping, WLAN, distributed client, data aggregation, bandwidth priority access, traffic control**

I. Introduction

Traffic shaping, also known as packet shaping, is the practice of regulating network data transfer to assure a certain level of performance, quality of service (QoS) [1]. The practice involves delaying the flow of packets that have been designated as less important or less desired than those of prioritized traffic streams. Regulating the flow of packets into a network is known as *bandwidth throttling*. Regulating the flow of packets out of a network is known as *rate limiting*. Traffic shaping is used for a number of purposes such as in a corporate environment; business-related traffic may be given priority over other traffic. For other functionality, traffic shaping could be an integral component of a two-tiered internet, in which certain customers or services would get traffic priority for a premium charge.

In a specific healthcare environment, a wireless medium, like WLAN, is considered promising for use in data transport [2]. Similar approach can also be adopted for the residential safety. WiFi uses the unlicensed ISM (Industrial, Scientific, and Medical) band centered at 2.4 GHz. Data rates above 11 MHz can be achieved; however, it is more typical to see data flow at 5 MHz or less. Fully computerized residential safety information systems are desired in Malaysia. A typical information system consists of server computers, terminals, a database, and a LAN. The idea of residential safety information system can provide quick communication between guards, policemen and residents with the immediate dissemination of criminal or emergency information. Installation of a wireless data communication system compatible with an emergency information system has been reported to improve efficiency [3]. Voice communication system is also necessary to transmit instructions quickly in emergencies, such as a sudden report of break-in and triggering alarm of a house. In order to attain an environment in which access and the sharing of information are possible anywhere and at all times, a telecom infrastructure with a mobile communications network is very important to voice and data communication. However, the allocated bandwidth to transfer such voice and data communication tends to fluctuate in mobile environment and this is bad for emergency situation when it has to be shared with other residents that use the network to get connected to internet. As an example, a patrolling guard might need to compete for the bandwidth with other users that are less urgent. In worst situation, the emergency data might fail to be transmitted due to the congested network.

In this paper, a system performance of selected traffic shaping technique is studied and reported. Based on the traditional bandwidth throttling traffic shaping, the technique is further enhanced and improved for residential safety dynamic environment. This is proposed as an adaptive bandwidth traffic shaping mechanism (ABTS). The conducted study was preliminarily simulated and later was taken into an actual environment to observe performance of the proposed mechanism.

The paper is organized as follows. In the next section, the proposed system architecture is described, and some background information of the mechanism is given. In Section III, the proposed system model is presented. Section IV depicts system methodology to illustrate the

Manuscript received September 5, 2013; revised August 1, 2014.

doi: 10.12720/lnit.2.2.141-145

efficiency of the algorithm. Simulation results are discussed in Section V. Finally, we conclude our paper in Section VI.

II. System Architecture

Based on the above WLAN description, proposed scenario in a wireless communication residential safety environment is best illustrated by Fig. 1. We can see from the diagram that major bandwidth resource is utilized by less priority application such as video streaming, Skype, Facebook, twitter, YouTube from the internet by many residents.

A. *Static Bandwidth Throttling*

Traffic shaping techniques were studied in order to solve the bandwidth competing issues between urgent and less urgent information among clients in a residential safety network. Bandwidth throttling traffic shaping technique [4] is a method of limiting the rate at which a bandwidth intensive device such as a server accepts data.

If this limit is not in place, the device can overload its processing capacity. Traditionally, there are two type of bandwidth throttling; namely static and dynamic. Static Bandwidth Throttling (SBWT) is similar conceptually to the hardware-based packet-shaping approach in that it targets a specific level of packet activity as its desired result.

A typical SBWT implementation would involve either a client-side or server-side setting that gates the amount of packet traffic generated or accepted at pre-configured (static) levels. Often these static levels are defined in terms of a percentage of available bandwidth (size of the pipe). In most cases, however, the pipe itself must be statically configured or declared. In other words, there is no real-time discovery of available bandwidth, and consequently, no reaction based on availability.

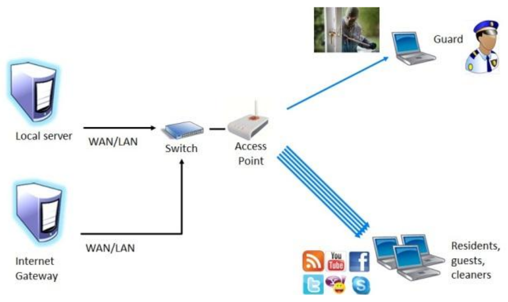

Figure 1. Scenario of system architecture in residential safety network

B. *Dynamic Bandwidth Throttling*

On the other hand, Dynamic Bandwidth Throttling (DBWT) is a more proactive approach and takes more parameters and consideration before deciding how much bandwidth should be allocated. Parameters such as quality of connection per user or per connection, application based are taken into account before decision is made [5].

However, DBWT regulates a bandwidth intensive device by limiting how much dynamic data that device can accept or receive. It does not limit the total transfer capacity, upstream or downstream, of data over a medium. Thus, having discussed our current scenario and problem, our proposed system is to modify such DBWT technique with an adaptive bandwidth capping mechanism from server to client with priority access control. This is best illustrated in Fig. 2.

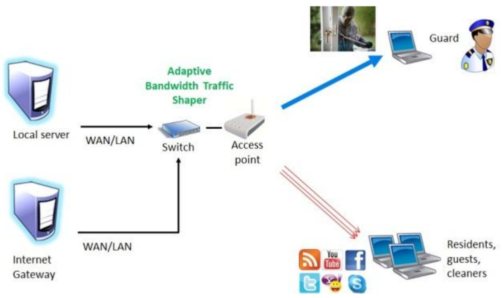

Figure 2. Proposed priority access dynamic bandwidth traffic shaping system architecture

In this proposal, the adaptive bandwidth traffic shaping algorithm is incorporated at the network switch.

Assuming the access point receives some information that is categorized as urgent and emergency, the priority of the available bandwidth will be given to the patrolling guard. This is controlled right from the server to ensure that the priority access is definitely allocated to the guard. When this is utilized, the less priority clients will be secondary and obtain remaining available bandwidth.

III. System Model

The above architecture is supported by the following system model shown in Fig. 3. Our adaptive bandwidth traffic shaping system model consists of six communication components which may reside in an access point. Source distributor identifies the origin and destination of the data from which server to which clients. Traffic monitoring unit observes the condition of the traffic in each traffic path and detect the deterioration of data occur in the most priority link. Once the data start to reduce in its quality, priority access controller will be triggered to enable data prioritization according to data class and its respective policies. Bandwidth classification will be assigned according to this priority control. Once it is classified, pre-agreed resource allocation will be given to each class. This is executed in resource decision maker. While assigning such bandwidth, assessment on the quality of the transmission will be conducted for record of the network historical performance.

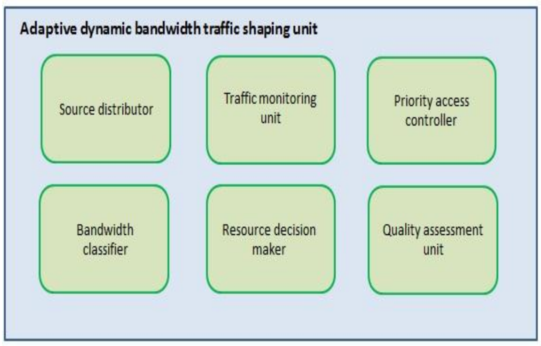

Figure 3. Adaptive dynamic bandwidth traffic shaping system

IV. System Methodology

In order to simulate such system architecture and system model, Fig. 4 details the steps of the conducted simulation program.

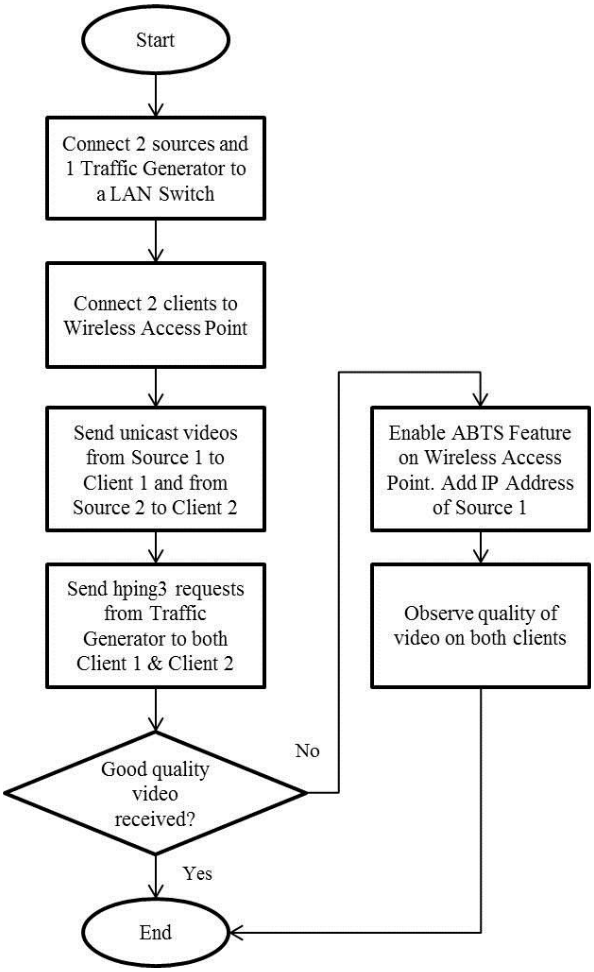

Figure 4. Simulation steps

In this study, two classes of clients are assumed, one is for the urgent information requestor and another one is for the less urgent requestor. Local server is setup to keep all the important information of the residents as well as past history information of residential safety. Another server is link to the internet.

For this simulation, two sources and a Linux machine set as a Traffic Generator are connected to a LAN switch. The two clients are connected wirelessly to the Wireless Access Point that has the ABTS feature.

Once the sources and clients have been set up, unicast videos are sent from Source 1 to Client 1 and from Source 2 to Client 2 respectively. At this point of time, there are two clients connected to the Wireless Access Point and hence not much traffic is observed. The simulation then uses hping3 application that sends hping3 requests to the network. This application will generate enough traffic that can flood the network. Once the network is congested, it can be clearly seen that the videos on both the Client 1 and Client 2 have deteriorated. Quality of the videos can be really bad depending on the frequency of the ping requests sent by the hping3 application.

Next, the ABTS feature is enabled on the Wireless Access Point. Enabling the ABTS feature will add a traffic class specific for the priority source with the dedicated bandwidth assigned to it. Any data passing through the Wireless Access Point will be filtered according to this class and the specified bandwidth will be assigned to the priority source.

For example, during the simulation, Source 1 has been classified as a priority source and hence the ABTS is enabled for Source 1. Once ABTS is enabled, the quality of the video received at Client 1 will be good again compared to the video received at Client 2. This is because priority has been given in terms of bandwidth dedicated to Source 1 has enabled the video to be transmitted without any effect from the congested network.

V. Simulation Results

This section describes in detail simulation results of the study. Fig. 5 depicts the percentage of discarded data whenever the proposed Adaptive Bandwidth Traffic Shaping (ABTS) is enabled and disabled in the smart access point. As shown in the figure, it is obvious that, with ABTS enabled on each A (guard) or B (residents) clients path, the percentage of discarded data reduce tremendously as low as 0% compared to without the ABTS. However, ABTS is mostly useful when the link is congested such as many reported images need to be retrieved from local surveillance cameras. Hence for the case where ABTS is disabled, the percentage of data loss is almost 0% because the network is not congested. In the situation where network is congested, such mechanism will help to reduce any congestion or link error by giving priority of the bandwidth right from the backhaul (server). The percentage of discarded is highest when link B (e.g. residents using internet, Facebook, YouTube) is experiencing congestion while no ABTS functionality available. This may lead to a very serious problem when there is any emergency case occurs at this point of time. The guards may not be able to receive critical information and even can also lead to loss of connectivity if the traffic is too congested.

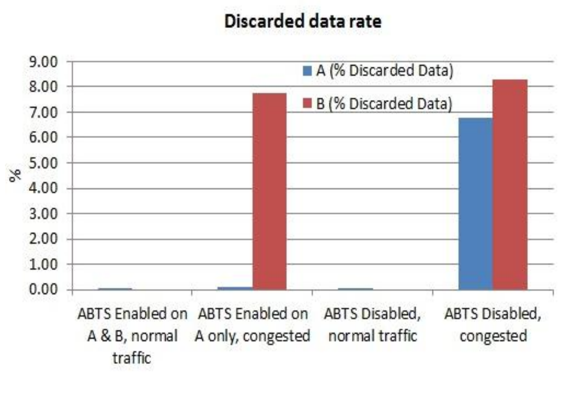

Figure 5. Percentage of discarded data with ABTS

Fig. 6 on the other hand, shows the system performance in terms of audio data lost when ABTS is deployed. This simulation is necessary to show how severe is the lost with and without the proposed ABTS. Since ABTS is about priority access and in this case priority is always given to A (guard) which require for transmission of emergency information, it can be observed that the highest audio data lost occurs at B when ABTS enabled during congested link situation and priority is given to A. This simulation results is concurrent with our previous Fig. 5 whereby during normal traffic regardless ABTS is on or not the audio data loss is hardly reduced or affected for A, and the percentage increases when ABTS is disabled during congestion.

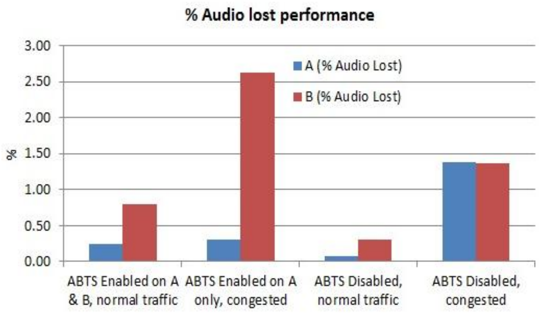

Figure 6. Percentage of audio data loss with ABTS

Fig. 7 further illustrates the ABTS performance on video data lost. Similar to audio, in video data the incorporation of ABTS to one of the server clients certainly reduces the amount of data lost during data congestion. Refer to the graph, the total reduction of data loss is nearly 60%. This improves the communication and capacity of the network during critical emergency cases. However, it can be seen that, on average the video data loss is more sensitive than the audio lost. Perhaps the video data is more susceptible to the interference.

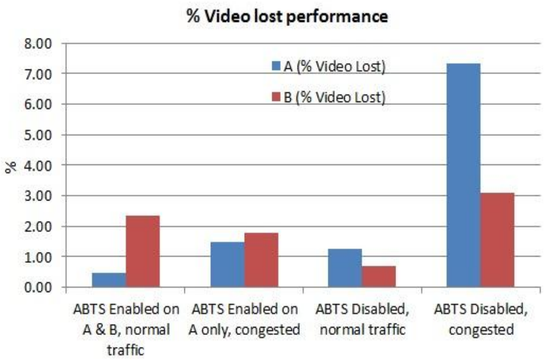

Figure 7. Percentage of video data loss with ABTS

In the example scenario of residential safety, this is quite critical since emergencies can happen during the time when traffic is most congested. Loss of audio or video can lead to serious implications.

Other scenarios that can utilize this traffic shaping mechanism proposed are corporate, healthcare or campus environment [6] where there is high number of users and also when there is a need of propagating critical information to critical users in certain conditions. This critical information can be susceptible to data loss during network congestion and hence is unacceptable in certain situation such as emergency.

VI. Conclusions

Simulation results have shown that the proposed adaptive bandwidth traffic shaping mechanism improves the performance of the clients during data congested situation. Priority access is given to the server which holds critical information. Hence the clients who are in need of information during emergency and safety situation will not experience loss of data during this critical situation since dedicated bandwidth is assigned to the critical server. Our preliminary results only proof the technique can reduce the amount of data discarded either for video or audio data. Further analysis need to be conducted especially when dealing with multi class priority access and the actual link quality. More traffic shaping mechanisms can also be implemented such as limiting uploading and downloading of data to users that are not critical in the system.

References

[1] M. Rouse. (June 2010). Traffic shaping (packet shaping). *IEEE Trans. Plasma Sci.* [Online]. Available: www.searchnetworking.techtarget.com

[2] B. Senese, "Implementing wireless communication in hospital environments with bluetooth, 802.11b, and other technologies," *Medical Device and Diagnostic Industry*, July 2003.

[3] E. Hanada, S. Tsumoto, and S. Kobayashi, "An ubiquitous environment through wireless voice/data communication and a fully computerized hospital information system in a university hospital," *IFIP Advances in Information and Communication Technology*, vol. 335, no. 1, pp. 160-168, 2010.

[4] C. Foley. (2002). Dynamic Bandwidth Throttling – A Technical White Paper, pp. 1-11. [Online]. Available: http://www.mobileinfo.com/WhitePapers/XcelleNet_Dynamic%20Bandwidth%20Throttling%20White%20Paper_Final.pdf

[5] IBM Tivoli Endpoint Manager Version 8.2. (Aug 2013). [Online]. Available: www. pic.dhe.ibm.com/infocenter/tivihelp/

[6] B. Comp. (2013). Healthcare System Secures Enhanced Network Communications [Online]. Available: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/case_study_c36-726508.pdf

Putri S. Khalid received her bachelor degree in Electrical & Electronics Engineering from University of Queensland, Australia in 1998. She started her carrier in the field of microelectronics design. She then gained her experience in embedded design for various fields such as telecommunication devices, information security and later wireless network solutions. She has been in MIMOS Berhad since 2008 as a researcher as well as a developer. She is now working on wireless access network and also mesh network solutions. She has filed several patents in the area of information security and wireless network and looks forward to being able to implement solutions that can benefit the community.

Wahidah Hashim received her bachelor degree in information technology, business management and language from University of York, UK in 1999. She then pursued her MSc in Multimedia Technology at University of Bath, UK in 2001. She completed her PhD studies from King’s College London, UK in 2008 in the field of Telecommunication Engineering. She is currently working at MIMOS Berhad wireless communication cluster as a staff researcher since 2009.Apart from her main task in doing research in cognitive radio, WLAN, OFDM, space-time coding, MIMO systems and wireless system, she is actively involved in the development of Malaysia technical specification, standard and guidelines of wireless terminal devices, International Mobile Telecommunication (IMT) systems and wireless sensor network for Malaysia Communications and Multimedia Commission (MCMC). She has occasionally represented Malaysia at International Telecommunication Union (ITU) working party 5D meeting for IMT-Advanced technology. Dr. Wahidah has published several publications and filed several patents on her research findings. She is a member of the IEEE.