ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

A Secured and efficient technique of Multicast Admission Control Mechanism for IPTV

Ahmed Bakal

Abstract*—Recently, the developments in high-speed networks and the evolution in digital video broadcasting techniques have made IPTV possible today. IPTV still has risks, threats and vulnerabilities that should be overcome such as identification, authentication and content encryption. IP multicast technology is used to provide IPTV service. In a multicast environment, common problems such as message authentication and privacy became more complex. Other concerns are introduced by the multicast environment such as the access control of the group, trust of the group and trust of the router. These concerns are further complicated by the group membership dynamic nature due to joining/leaving the group. In this paper, a security mechanism is proposed and implemented to provide security to the IPTV service. Group Encrypted Transport VPN (GETVPN), which is originally proposed by Cisco to use in enterprises is applied here to secure IPTV environment. Emulation of an IPTV network is made using GNS3, VMware workstation, Cisco OS and VLC program. The proposed security solution is applied; as a proof of concept video is streamed from the sender to the receiver successfully implementing our proposed solution.

***Keyword*–IPTV; Security; Admission control; VPN; GDOI.**

I. INTRODUCTION

Before about 80 years, television was invented that has shaped the way culture and society has evolved. With the foundation of Advanced Research Projects Agency Network (ARPANET) in 1969, a new stage in communication has been started.

Due to several common similarities between the Internet and television and the huge growth of broadband networks, this make the current trend is to turn into the concept of 'All-over-IP'.Where in most service platforms will be changed into a single IP-based platform. Thus, creating Internet Protocol Television (IPTV) become a reality.IPTV can be explained as digital video content, which is sent via the use of the Internet Protocol (IP). This IPTV definition is very simple and it excludes the Internet from playing a role in the delivery of any type of television and video content. [1]. IPTV deployment has many problems such as content encryption, authentication, authorization and key distribution. Overcoming all the security issues in IPTV is a complex job. Thus, there are some problems that have not been resolved yet. [2]:

- A trade-off between risks and complexity should be made by security professionals to reduce the effect of both of them.
- VPN is considered a good solution for many applications; however, it is considered not suitable for IPTV because of its overhead.
- Techniques such as encryption and integrity-protection are needed to prevent a network from Denial of Service (DoS), Distributed Denial of Service (DDoS) or similar kind of attacks.

In this work, VPN has been implemented after some modifications because designing VPNs, especially for an IPTV environment, remains an open problem. The modifications aim to decrease the overhead and at the same time keep the delay at an acceptable values. The results obtained declare this claim.

Confidentiality and integrity techniques also considered an open research issues. As part of our work, encryption, authentication and authorization have been used through the implementation of IPsec, Advanced Encryption Standard (AES) algorithm, hash algorithm and other techniques.

II. LITERATURE REVIEW

A.Adewale and et al, [1] make a comparison of Virtual Private Network (VPN) and Dynamic Multipoint Virtual Private Network (DMVPN) illustrating the benefit of using DMVPN and proving that it is a highly scalable VPN technique with minimal configurations and robustness. In the proposed work, VPN and DMVPN are tested and state the benefits and drawback of both of them and prove that these mechanisms are not suitable for IPTV environment.

In knowledge base website, Group Domain of Interpretation (GDOI) based Dynamic Multicast Virtual Private Network (DMVPN) is used, in which tunnels were implemented to pass through other networks with separate key server. The key server is configured to distribute keys in unicast fashion; the proposed design in our works does not need to establish tunnels to communicate between routers.

G.Witherspoon and et al, [2] outlined a network-based approach Group Domain of Interpretation (GDOI) for solving access control issues.

T.Bartczak and P.Zwierzykowsk [3] try to evaluate the performance of the two Source Specific Multicast (SSM) protocols for IP networks: PIM SSM and Lightweight PIM (LPIM). LPIM limits the number of signaling messages and processing overhead related to handling of the associated state machines. The routing protocol used in this work is the ordinary PIM protocol because it is certified and widely used in contrary to LPIM which is still in draft stage.

They have analyzed the security aspects of the new Key Management Protocol (KMP) proposed by the Keying and Authentication for Routing Protocols (KARP) working group of the Internet Engineering Task Force (IETF). These protocols are formally validated using the AVISPA modeling tool. The proposed work is using GDOI key management protocol.

Manuscript received: 20 February 2019
Manuscript received in revised form: 19 March 2019
Manuscript accepted: 03 April 2019
Manuscript Available online: 10 April 2019

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

III. IPTV DEPLOYMENT PROBLEM

Large-scale IP-multicast deployment has not been seen at Internet Service Providers (ISPs). And so on, IPTV services will be a major driver of future IP multicast deployments. This means the capability of end-to-end Quality of Service (QoS), accounting, and the availability of a service, beside the support of multicast layer 3 VPNs and multicast MPLS.

For IPTV services, multicast is better way to provide QoS, but there are two problems with multicast:

The new Applications and technologies such as IPTV now require immediate communication from branch-to-branch.

- The dynamic nature of multicast group make it harder to apply standard encryption and authentication infrastructures.

Also, IPTV environment suffers from many security-related issues; Applying security to overcome all these issues will increase complexity on the network and will make it difficult to the service provider to deliver the required level of service. Hence, while designing such a secure system a trade-off between the risks and complexity should be taken into account. In other words, a balance between risk reduction and expected costs should be made. Applying of VPN to secure IPTV network is another problem because of its overhead. The using of tunnel-based encryption solutions such as IPsec/GRE and DMVPN are all point-to-point. They are require the supplying of a complex connectivity mesh in order to apply in IPTV network.

The main areas of concern in designing a secure system are [1]:

- The equipment used in networking and communication that link the display to the data source.
- The equipment that are related to IPTV environment are used to operate the IPTV service and information and enable it to operate.

IV. SIMULATION COMPONENTS

The following components are used in the emulation model of this work are:

- Graphical Network Simulator 3(GNS3) version 1.4.6
- VMware workstation version 10.0.1
- Cisco routers c2600.
- Cisco IOS Software Release 12.4(15)T
- Windows XP professional
- VLC media program

GNS3 is used to make the simulation where an image of c2600 Cisco router is added in GNS3 of version 12.4(15)T. Instead of using a separate computer or laptop to act as the sender and the receiver, VMware workstation is used to install virtual windows XP professional to work as sender and receiver. VLC program is installed on Windows XP to stream the video in the sender and to play the stream in the receiver.

V. THE PROPOSED SOLUTION

In this work, VPN has been implemented to provide access control to the IPTV network along with cryptography and data integrity. This VPN have some modifications that will decrease the overhead caused by regular VPN techniques, and at the same time keeping the delay at an acceptable values. The results obtained declare this claim. As part of our work, encryption, authentication and authorization have been used through the implementation of IPsec, AES algorithm, hash algorithm and other techniques.

Group Encrypted Transport VPN (GETVPN)is applied in the simulation to secure IPTV network. GETVPN introduces the concept of trusted group to eliminate tunnels that are point-to-point and their related overlay routing. A mutual Security Association (SA) is established between all the group members (GMs), which is known as a group SA. This gives the ability to any GM in the group to decrypt traffic, which is encrypted by another GM.

GETVPN is a set of features needed to protect a multi-channel traffic that passes through a Cisco system through a private WAN. GETVPN fuses the Interpretation Domain (GDOI) Community, the IP Security keypad protocol (IPsec) enabling an efficient way to secure traffic for users. GETVPN allows the router to enforce non-tunneled ("native") IP encryption and removes the need for tunnel configuration.

The solution of GETVPN relies on free and creative technologies patented by Cisco. In order to provide the necessary features GETVPN, besides the support of existing IKE, IPsec and MultiCast technologies, uses the following basic components [6]:

- Group Domain of Interpretation(GDOI)
- Key servers (KSs).
- Cooperative (COOP) KSs.
- Group Members (GMs).
- IP tunnel header preservation
- Group security association.
- Rekey mechanism.
- Time-Based Anti-Replay (TBAR).
- Interoperability (IP-D3P).

In this work, a network scenario has been made to emulate an IPTV network starting from the content provider to the end user. An admission control solution has been proposed and implemented in this emulation as well as three different security solutions. Scenarios 1 to 3 highlighted the problems in each solution while scenario 4 tries to capture the benefits and extracts the issues that bring problems in the proposed solution. A comparison between these cases is provided to prove that the proposed solution is an acceptable solution in terms of time and security.

A. Scenario 1: IPsec VPN

VPN is a technology that enables information to be protected via a public network. It permits users to set up a virtual private tunnel for safe access through an insufficient network [6] to an intimate network to an internal network. IPsec VPN is not multicast secured by IPsec [6]. The

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

purpose of this work is to protect multi-cast traffic. Network topology as shown in Figure 1.

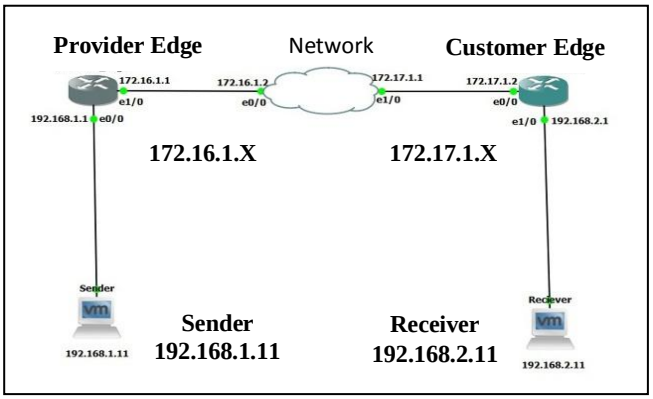


Fig.1: IPsec VPN topology

After running the simulation scenario, the IPsec SA and ISAKMP Security Association (SA) is established between PE router and CE router a prove that IPsec VPN has not been used to secure multicast (which is a problem). Multicast data is sent through Trace command from the sender gateway (192.168.1.1) to the receiver gateway (192.168.2.1) in the multicast group. Figure 2 shows the reverse path of the multicast traffic from the receiver to the network router and then to the sender, not passing through VPN tunnel**.**

```
PE#mtrace 192.168.1.1 192.168.2.1 239.1.1.1
Type escape sequence to abort.
Mtrace from 192.168.1.1 to 192.168.2.1 via group 239.1.1.1
From source (?) to destination (?)
Querying full reverse path...
 0  192.168.2.1
-1  172.17.1.2 PIM  [192.168.1.0/24]
-2  172.17.1.1 PIM Reached RP/Core [192.168.1.0/24]
-3  172.16.1.1 PIM  [192.168.1.0/24]
```

Fig.2: Trace route from the sender to the receiver in scenario 1

B. Scenario 2: VPN over GRE tunnel

Site-to-site VPN is implemented with IPsec and Generic Routing Encapsulation (GRE) . GRE will solve the problem of scenario one because it allows to tunnel unicast, multicast and broadcast traffic between routers and are often used for routing protocols between different sites. The problem with GRE tunneling is that it does not provide any form of protection to the transferred data, thus IPsec is used along with GRE to secure the entire GRE tunnel. This allows having a secure and safe site-to-site tunnel. Thus, the multicast data used for IPTV can be secured using the tunnel. Figure 3 shows the topology of the simulation. The topology looks the same as the previous scenario but the configuration is different because GRE tunnel is used alongside with IPsec.

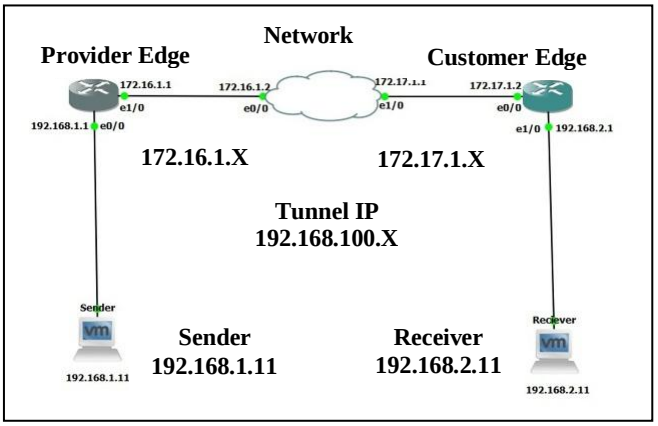


Fig. 3: IPsec over GRE topology

After running the simulation, The IPsec Security Association is established between the tunnel edges. The difference between this scenario and the previous one (section A) is that multicast data have not been protected by IPsec in scenario one. In scenario two the combination of GRE tunnel and IPsec that allow to secure the transfer of unicast, multicast and broadcast. The combined GRE tunnel and IPsec can secure IPTV multicast service.

Figure 4 shows the reverse path of the multicast traffic from the receiver gateway (192.168.2.1) to the tunnel interface at the receiver side (192.168.100.2) to the tunnel interface of sender side (192.168.100.1) and then to the sender (192.168.1.1), thus the multicast traffic is transferred from the sender through the GRE tunnel and protected by IPsec. This solution solve the problem of scenario 1.

```
PE#mtrace 192.168.1.1 192.168.2.1 239.1.1.1 10
Type escape sequence to abort.
Mtrace from 192.168.1.1 to 192.168.2.1 via group 239.1.1.1
From source (?) to destination (?)
Querying full reverse path...
 0  192.168.2.1
-1  192.168.100.2 PIM/Static  [192.168.1.0/24]
-2  192.168.100.1 PIM  [192.168.1.0/24]
-3  192.168.1.1
PE#
PE#
```

Fig.4: Trace route from the sender to the receiver in scenario 2

The problem with this scenario is that, if it is applied in an IPTV environment, a GRE tunnel should be established between the content provider (sender) and each access router (edge router near the receiver) which is considered impractical for transferring IPTV. This problem has been overcome in the paper with the proposed solution.

C .Scenario 3: Dynamic Multipoint VPN (DMVPN)

The DMVPN is a safe network that traffic-free exchanges between sites through the VPN server or router of a company headquarters. The mesh VPN topology is essentially formed. This means that any site (speaker), no matter where they are located, will link directly to all other sites. DMVPN uses GRE multipoint tunneling and thus generates a tunnel with IPsec SA for every branch of the network. Figure 5 shows DMVPN's network topology.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

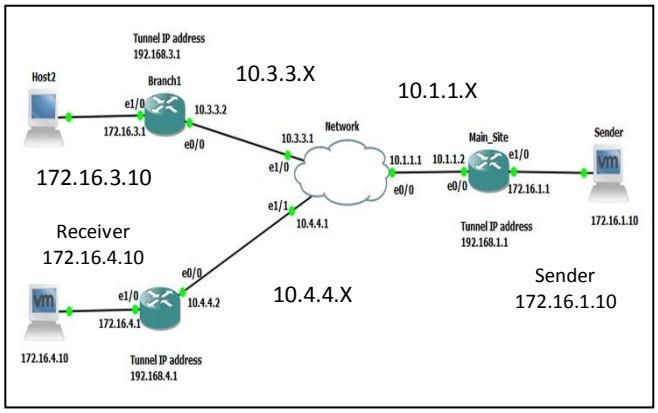


Fig. 5: DMVPN network topology

The problem in scenario two has been solved in this scenario through establishing a Multipoint GRE tunnel to each receiver wishes to receive IPTV service. However, this solution is not recommended for transferring real time voice and video traffic used in IPTV. It requires a long time to transfer data, which is not suitable for real time IPTV service

The traffic send from the sender (172.16.1.10) to the receiver (172.16.4.10) that is a member in the group (239.1.1.1). Figure 6 shows the reverse path of the multicast traffic from the receiver (172.16.4.10)to the tunnel interface at the receiver side (192.168.1.4) to the tunnel interface of sender side (192.168.1.1) and then to the sender (172.16.1.10) which proves that the multicast traffic is going through the tunnel and secured by IPsec through the tunnel.

```
MS#mtrace 172.16.1.10 172.16.4.10 239.1.1.1
Type escape sequence to abort.
Mtrace from 172.16.1.10 to 172.16.4.10 via group 239.1.1.1
From source (?) to destination (?)
Querying full reverse path...
 0  172.16.4.10
-1  192.168.1.4 PIM  [172.16.1.0/24]
-2  192.168.1.1 PIM Reached RP/Core [172.16.1.0/24]
MS#
```

Fig. 6: Trace route from the sender to the receiver in scenario 3

In order to check the delay in this scenario, a simple traffic is sent from the sender to the receiver belonging to a multicast group. A repeated multicast ping is performed where each ping is of size (17000 byte); the replays from the receiver have been recorded as shown in table 1.

D. Scenario 4: GETVPN

A separate Key Server (KS) is added to the network. It is responsible of all the encryption policies used in the network, such as traffic, encryption protocols, security association, rekey timers, Access Control List (ACL) and so on, all are defined centrally on the KS and are pushed to all GMs at the registration time. KS run GDOI key management protocol. The configurations of the KS include: defining the IP address of the used interface, enabling them, configuring the unicast routing protocol (OSPF), defining multicast routing protocol (PIM-SM) and defining the Rendezvous Point (RP), (172.16.1.2), defining IKE phase 1, defining IPsec configuration, Generating RSA keys, defining GDOI group, defining rekey parameters and Access Control List.

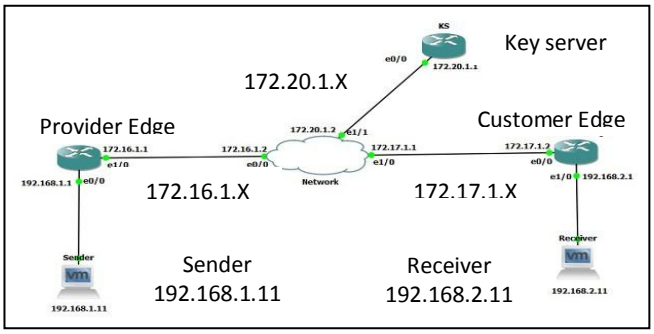


Fig. 7: Network topology of the proposed solution

Each router in the network should be configured as GDOI group member in the established group SA. The configurations include: defining the IP address of the user interfaces, enabling them, configuring the unicast routing protocol (OSPF), defining multicast routing protocol (PIM-SM), defining the Rendezvous Point (RP), (172.16.1.2), defining IKE phase 1, GDOI group, crypto map and applying this to the interface toward the network.

After configuration is done, each group member in the network registers to the key server and become members in the group as shown in figure 8. The Key Server authenticates Group Members (GMs), the key server uses Pre-Shared Key authentication method for this process (Password given by the operator). If authentication is successful, an IKE phase1 SA is established between KS and GM which used to protect GDOI. Then, GDOI establishes rekey and data security SAs.

Two keys are received in each GM from the KS, the first is Key Encryption Key (KEK), which is used to encrypt the control traffic, and the second is the Traffic Encryption Key (TEK), which is used to encrypt the data traffic. The KS performs rekey before existing keys expire in order to update the policy and keys used by the group member to encrypt or decrypt traffic.

```
%CRYPTO-5-GM_REGSTER: Start registration to KS 172.20.1.1 for group GDOI-GROUP1 using ad

%CRYPTO-6-GDOI_ON_OFF: GDOI is ON
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group GDOI-GROUP1 transitioned to Unicast Rekey.
%GDOI-5-GM_REGS_COMPL: Registration to KS 172.20.1.1 complete for group GDOI-GROUP1 usin
```

Fig. 8: Registration process of PE to the KS

After registration is completed, Group Members can communicate securely between each other. Sender should be configured in order to stream the video. IP address should be configured and the routing protocols. The sender uses VLC media player to stream the video. Instead of using a separate computer or laptop, a VMware workstation is

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

used to install virtual windows XP professional. VLC program is installed as well on this virtual windows. The configuration in the sender include specifying the IP address of the interface, specifying the video to be send, Specifying the transport protocol (RTP/MPEG Transport protocol), transcoding options and specifying the multicast group address in which the sender will stream the video

The receiver should be ready to receive the streamed traffic through a correct configuration. receiver IP address should be configured as well as the routing protocols. The most important configuration step is configuring the membership of the group. The receiver uses VLC media player to play the video. Instead of using a separate computer or laptop, a VMware workstation is used to install virtual windows XP professional. VLC program is installed as well on this virtual windows.

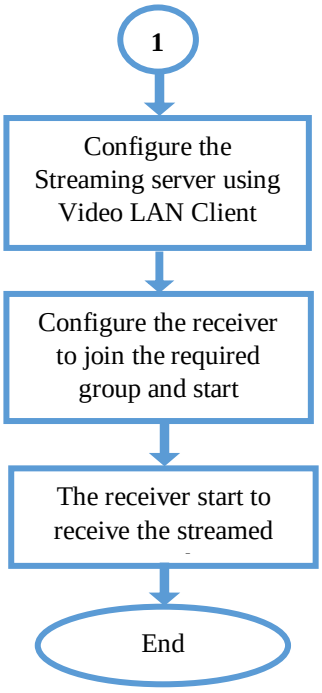
After completing the configuration in the receiver correctly, it will receive the streaming send by the sender; besides any end user owns a membership can join the multicast group and receive the stream. Now, the complete IPTV multicast scenario is performed successfully.

Another work is done besides the previous work in order to check the delay, a simple traffic is sent from the sender to the receiver belonging to multicast group, a repeated multicast ping is performed each ping is of size (17000 byte). The delay of each ping is as shown in table 1.The process flow of the proposed solution is shown in figure 9.

VI. RESULTS AND DISCUSSION

As shown in figure 10, 11 respectively. The sender will stream the video and the receiver will start to receive the streaming successfully through the proposed secured solution; IPTV stream is protected by IPsec, which is established under the protection of TEK, which is sent by the KS. The rekey is protected by KEK. Thus, the complete IPTV multicast scenario is performed successfully.

As shown in figure 12, security is achieved in PE router using GDOI, so as the other routers in the topology.



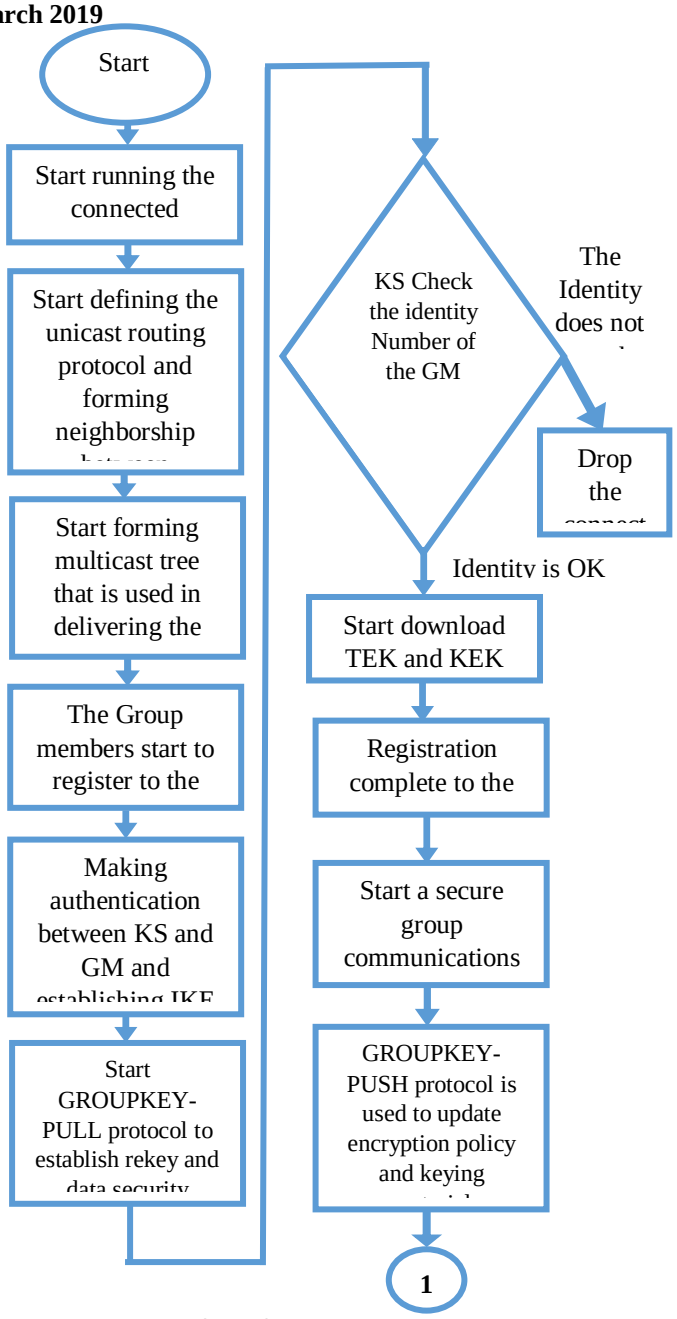


Fig. 9: The process flow of the proposed solution

In addition, a simple traffic (15-repeated multicast ping) is sent from the sender to the receiver applied in scenario 3 and scenario 4, and the replay time is recorded, and a comparison between them is done as shown in table 1 and figure 13.The proposed security solution does not cause any extra delay to the network that will affect the streaming.

The proposed solution resolves the problem of scenario one, which cannot protect multicast traffic and the problem of scenario two where a tunnel is required to each destination, which is impractical in multicast and in IPTV service. In addition, it solves the problem of DMVPN in which it takes more time to transfer data.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

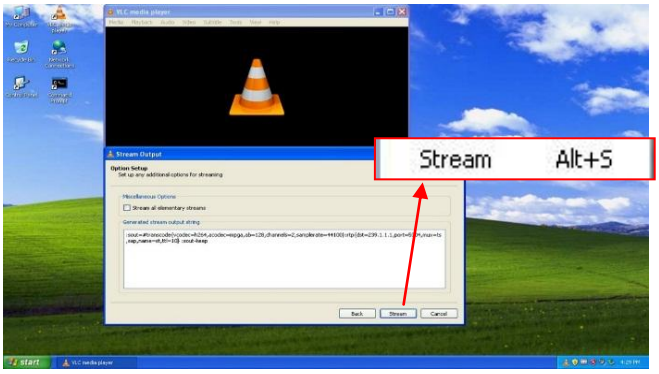


Fig. 10: Streaming video from the sender

Deployment of IPTV service faces specific threats and risks such as authentication, content encryption, key distribution, etc.

A security mechanism is needed to secure IPTV. In this work, VPN has been implemented after some modifications. The modifications aim to decrease the network overhead and at the same time keeping the delay at an acceptable value. Key Server is added to the network provider with GDOI keying protocol to achieve an admission control mechanism for securing IPTV network.

Fig. 11: Receiving the stream in the receiver

Table 1: replay time (in milliseconds)

Ping Sequence	DMVPN	GETVPN
1	79	50
2	98	71
3	96	60
4	94	47
5	91	34
6	87	43
7	105	62
8	101	55
9	102	67
10	100	44
11	105	51
12	84	51
13	96	57
14	100	57
15	115	54

```
PE#sh crypto gdoi
GROUP INFORMATION

    Group Name               : GDOI-GROUP1
    Group Identity           : 999
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 172.20.1.1
    Group Server list        : 172.20.1.1

    GM Reregisters in        : 6779 secs
    Rekey Received           : never


    Rekeys received
         Cumulative          : 0
         After registration  : 0
    Rekey Acks sent          : 0

ACL Downloaded From KS 172.20.1.1:
   access-list  deny udp any port = 848 any port = 848
   access-list  deny tcp any any port = 49
   access-list  deny tcp any port = 49 any
   access-list  deny tcp any any port = 179
   access-list  deny tcp any port = 179 any
   access-list  deny ospf any any
   access-list  deny eigrp any any
   access-list  deny udp any any port = 123
   access-list  deny udp any port = 123 any
   access-list  deny udp any any port = 161
   access-list  deny udp any any port = 161 any
   access-list  deny udp any any port = 514
   access-list  deny udp any port = 514 any
   access-list  deny pim any any
   access-list  permit ip any any

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86399
    Encrypt Algorithm        : AES
    Key Size                 : 128
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
 Ethernet1/0:

 IPsec SA:
     spi: 0xF8E1D03B(4175548475)
     transform: esp-aes esp-sha-hmac
     sa timing:remaining key lifetime (sec): (7126)
     Anti-Replay(Time Based) : 5 sec interval
```

Fig.12: PE registration in GDOI group

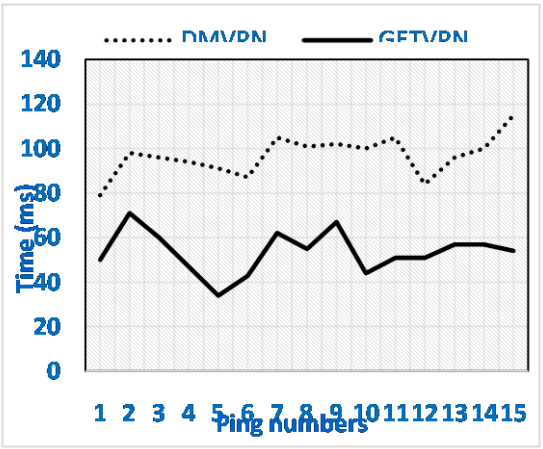


Fig.13: Comparison between DMVPN and GETVPN in terms of replaying time to ping commands

An emulation of an IPTV network is made using GNS3, VMware workstation, Cisco OS and VLC program. The proposed security solution is applied; Video is streamed from the sender to the receiver successfully implementing

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 8, Issue 9, March 2019

our proposed solution. In the proposed scenario, multicast type of communication has been used, where the operator streams the video to selected users those subscribed to a group. This way decreases the network overhead caused by many subscribers besides the charging will be lower because the cost is distributed amongst the group members.

The proposed solution has provided security to IPTV traffic transferred from the sender to the receiver.

VII. CONCLUSION

IPTV excludes the Internet from playing a role in the delivery of any type of television and video content. IPTV adds personalized and interactive options in viewing television program as compared to the traditional satellite TV- cable based.

In real-time applications such as Virtual Reality, online gaming, and everything that comes with 5G and Internet of Things (IoT), discussions are made about these applications. As a reference, the blink of an eye takes about 150 milliseconds. In voice communications, echo will be noticed when delays exceed 150ms. These benchmarks or metrics define how real-time applications should transfer and react with humans [6].

The proposed solution does not add an extra delay to the stream, which is shown and proven by comparison with other methods (figure 12).The reply time of the ping shows that the network is suitable for transporting IPTV service, besides it solves the problem of scenario three which protect the network through the use of tunnels. The replay time for the ping recorded in the proposed scenario GETVPN (scenario 4) is half that of DMVPN (scenario3) which is suitable for delivering IPTV service.

REFERENCES

[1] A. Adewale, V. Mathews, C. Ndujiuba and A. Adenrele. "Reduction of Routing Delay in an Enterprise Network using Dynamic Multipoint Private Network". International Journal of Computer Applications, vol. 179, no. 9, pp. 1-6,2018.

[2] G. Witherspoon, K. Quock, C. Peterson, A. Aggarwal, D. Gilbert and B. Hamilton, "Securing Enterprise Multicast Access Control Requirements with Group Domain of Interpretation". IEEE Military Communications Conference, USA , pp:1411-1415,6-8 Oct. 2014.

[3] T.Bartczak and P. Zwierzykowski, "Performance Evaluation of Source-Specific Multicast Routing Protocols for IP Networks". 8th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing, Poland, pp:1-6, 18-20,July 2012.

[4] Y. Huang and J. Atwood. "Security Analysis of Multicast/Unicast Router Key". IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), Canada, pp:1-6, 13-16 May 2018.

[5] A. Yadav and S. Soni. "Rekey Distribution for Multicast Key Environment". Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 687-697, 2017.

[6] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor and B. Pinkas "Multicast security: a taxonomy and some efficient constructions," IEEE, New York, NY, USA, pp:1-21,1999.

[7] P. Judge and M. Ammar. "Security Issues and Solutions in Multicast Content Distribution: A Survey," IEEE networks, pp. 30-36, January/February 2003.