VIDEO COMMUNICATION OPTIMIZATION IN MANET

Jyoti chhikara[*]

Sunita Dixit[**]

Abstract:

A Mobile Ad Hoc Network (MANET) is composed of mobile nodes without any infrastructure like wireless access points or base stations. Recent advances in computing technology, encoding schemes, high link bandwidth and high-speed networks have made it feasible to provide real-time multimedia services over the Internet. Video Transmission with high resolution increases the network traffic that can result the packet loss over the network. The situation becomes more critical when the network is having some attacker node that performs the flooding so that that the networks delay is increased over the network. To achieve the effective communication in such attacked infected clustered mobile network, an attack preventing routing scheme is suggested in this paper. To provide the effective communication over this delayed mobile network, a distinctive multipath based data chunk sequencing scheme is suggested in this paper.

Keywords: attacks, MANET, video streaming, packet loss.

[*] Student, CSE Deptt, PDM College of Engineering for Women

[**] Asst Prof, CSE Deptt, PDM Collegeof Engineering for Women

I. INTRODUCTION

Mobile computers, such as PDAs and laptop computers with multiple network interfaces are becoming very common these days. Many of the applications that run on such devices involve multimedia, such as video conferencing, audio conferencing, watching live movies, sports, etc. Streaming multimedia over wireless networks is a challenging task. Extensive research has been carried out to ensure a smooth and uninterrupted multimedia transmission to a Mobile Host (MH) over wireless media. Recent advances in computing technology, encoding schemes, high link bandwidth and high-speed networks have made it feasible to provide real-time multimedia services over the Internet. Real-time multimedia, has timing constraints. The feature of playing back audio or video in real time over the internet is called multimedia streaming. For example, audio and video data must be played out continuously. If the data does not arrive well in time, the playout process will pause, which is very annoying to human ears and eyes. Real-time transport of live video or stored video is the predominant part of real-time multimedia. Multimedia streaming applications have their own specific requirements described as follow.

- Bandwidth

To achieve acceptable perceptual quality, a streaming application should typically have minimum bandwidth requirement. For video streaming, congestion control takes the form of rate control, i.e. adapting the sending rate to the available bandwidth in the network.

- Delay

Streaming media has limited end-to-end delay so that packets can arrive at the receiver in time to be decoded and displayed. If a video packet does not arrive in time, the playout process will pause, which is annoying to human eyes. A video packet that arrives after its playout time is useless and can be regarded as lost. To reduce the effect of time-varying delay in the network and to provide continuous playout, a playout buffer is generally used at the receiver side.

- Loss

Packet loss is unavoidable in the Internet and can distort audio or video quality, which is not acceptable. So, it is desirable to make a multimedia stream robust to packet loss. Multiple description coding is such a compression technique to deal with packet loss.

- Simple playout function

Streaming applications like VoD (video on demand) or online music require playout functions, for ex- stop, pause/resume, fast forward, fast backward, and random access.

- Decoding complexity

Today is the world of mobile device like cellular phones and personal digital assistants (PDAs) which require low power consumption. Therefore, streaming applications for these devices must be simple and have low decoding complexity is desirable.

II. RELATED WORK

According to [1], attacks on ad hoc networks generally fall into two categories: routing-disruption attacks and resource-consumption attacks. Much progress has been made in securing ad hoc networks against these attacks recently; however, none of them considers dropping attacks exploiting cross-layer knowledge. In paper [2], a novel scheme for Detecting Blackhole Attacks in MANETs (so- called DBA-DSR) is introduced. The blackhole problem is detected and avoided by BDA-DSR protocol, before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes. according to simulation results, the proposed DBA-DSR scheme outperforms DSR in terms of packet delivery ratio and network throughput. Existing selective encryption approaches [3-5] have been effectively applied to different multimedia codec’s such as MPEG1, MPEG2, MP3, MPEG4, H.264, etc. One of the first approaches to partial encryption was proposed by Meyer and Gadgast [5] in 1995 for MPEG-1 bit streams. The principle data to be secured included: all the headers, I frames, and I blocks. They proposed a number of combinations of the above scheme to attain different levels of security. Kachirski and Guha [6] proposed a cluster-based Intrusion detection system using mobile agent technologies. The proposed system uses mobile agents each performing a particular role. The results of each node are aggregated in cluster points in order to limit the packet monitoring task in a few nodes and minimize the IDS-related processing time by each node. Huang et al. [7] proposed a mechanism that needs separate monitoring nodes, specifically one monitor per cluster (nodes that are in one-hop range form a cluster). Monitors should be active for this approach. If there is one monitor per cluster, the monitor does most of the work. It may happen that monitor nodes run out of energy before the network does or before the network gets partitioned.

III. VIDEO COMMUNICATION OPTIMIZATION TECHNIQUE

Video Transmission with high resolution increases the network traffic that can result the packet loss over the network. The situation becomes more critical when the network is having some attacker node that performs the flooding so that that the networks delay is increased over the network. To achieve the effective communication in such attacked infected clustered mobile network, an attack preventing routing scheme is suggested here. To provide effective communication over this delayed mobile network, a distinctive multipath based data chunk sequencing scheme is suggested in this paper. The presented work is divided in three main stages.

- In first stage, the optimized route between the source and destination is identified. This identification is performed based on delay and loss analysis.
- Once the optimized route is identified, the next stage is to identify the substitution node of all intermediate nodes between source and destination. By performing the optimum threshold analysis, multiple routes are generated between source and destination. The identified multiple routes will not share any common intermediate node. In this stage, the attacker node identification will be done at the initial stage, the node having the delay more than threshold value will be treated as the attacker node or the delay node. After this stage, N number of attack preventive routes will be identified.
- Now to start the actual communication, in third stage, the video data will be converted to small chunks. The data chunks will be identified based on the available routes so that each route will get M data chunks. Finally, these data chunks will be send in parallel on multiple paths so that the network traffic will be distributed. At the receiver end, the data will be accepted from all these chunks and retrieved as the final video data. The presented work will be implemented in clustered network.

Flow chart of above suggested scheme is given below:

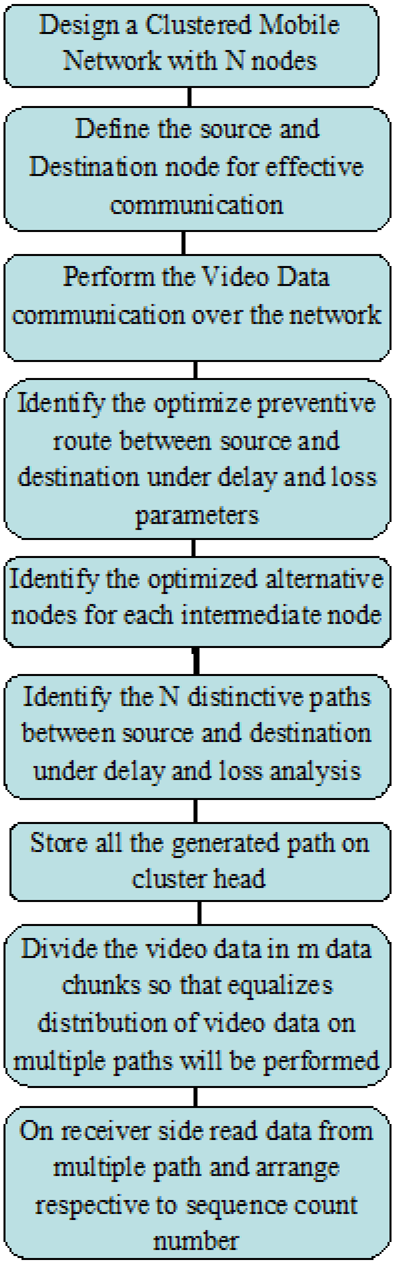
Design a Clustered Mobile Network with N nodes
Define the source and Destination node for effective communication
Perform the Video Data communication over the network
Identify the optimize preventive route between source and destination under delay and loss parameters
Identify the optimized alternative nodes for each intermediate node
Identify the N distinctive paths between source and destination under delay and loss analysis
Store all the generated path on cluster head
Divide the video data in m data chunks so that equalizes distribution of video data on multiple paths will be performed
On receiver side read data from multiple path and arrange respective to sequence count number

Fig1. Video optimization scheme

The suggested scheme is divided in following three main stages:

Stage 1: Optimized preventive route identification

At the earlier stage, the optimized attack preventive path will be identified between source and the destination. The route identification will be done under different parameters. The parameters included will be the loss analysis and delay analysis.

State 2: Distinctive Multipath identification

In this stage, the alternative for all intermediate nodes between source and destination will be identified. This alternative node identification will be done under the loss and delay analysis. Based on these nodes, the distinctive alternate paths between source and destination will be identified.

Stage 3: Parallel Video data Communication

In this stage, the video data will be divided in smaller data chunks and these data chunks will be communicated over multiple paths. This will perform parallel video communication over the network will be performed. At the receiver side these data chunks will be retrieved and sequenced to form the video data.

The significance of presented scheme is given here under

1. The presented scheme will use the distinctive path scheme so that the load over a specific node will not increase that will reduce the data loss.

2. It will identify the effective route based on communication analysis so that the attack preventive communication will be performed.

3. The parallel communication over the network will improve the effectiveness of communication.

IV. CONCLUSION

In this paper we have suggested an attack preventing routing scheme that will be implemented in ns2. To provide the effective communication over this delayed mobile network, this distinctive multipath based data chunk sequencing scheme is suggested. The presence of Dropping Attack affects all the parameters of network especially the throughput of the network affecting the Quality of multimedia data transmission. Proposed technique is very effective to detect and prevent the Dropping Attack. As this technique will use the distinctive path scheme so that the load over a specific node will not increase that will reduce the data loss.

V. REFERENCES

[1] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. IEEE Security and Privacy, 2(3):28–39, 2004.

[2] I.Woungang, “Detecting blackhole attacks on DSR-based mobile ad hoc networks”, International Conference on Computer, Information and Telecommunication Systems (CITS), 14-16 May 2012.

[3] J. Wen, M. Severa, W. Zeng, M. Luttrell, and W. Jin, “A format compliant configurable encryption framework for access control of multimedia,” in Proc. IEEE Workshop on Multimedia Signal Processing, pp. 435–440, 2001.

[4] A. M. Eskicioglu and E. J. Delp, “An overview of multimedia content protection in consumer electronics devices,” Signal Processing: Image Communication, vol. 16, pp. 681–699, 2001.

[5] T. Yuksel, “Partial Encryption of Video for Communication and Storage” Master’s Thesis, The Middle East Technical University, pp. 1-2, September 2003.

[6] O. Kachirski, and R. Guha, “Intrusion Detection Using Mobile agents in wireless Ad hoc Networks”, in Proceedings of the IEEE workshop on Knowledge Media Networking, pp.153-158, July 2002.

[7] Huang, Y. and Lee, W., .A Cooperative Intrusion Detection System for Ad Hoc Networks,. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN ’03), Fairfax, VA, October 2003.

[8] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. Rtp: A transport protocol for real-time applications, Internet RFC 3550, 2003.