www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6812-6816

Distinctive Multipath Based Data Chunk Sequencing Scheme

Jyoti Chhikara[1], Sunita Dixit[2]
[1]M.Tech student, PDM College of Engineering for Women
[2]Assistant Professor, PDM College of Engineering for Women
[1]Jyo.chhikara@gmail.com, [2]bhardwajsunita23@gmail.com

Abstract: A Mobile network is a hybrid network on which the different kind of data is communicated. One of the critical communicating data type over network is video transmission. Video Transmission with high resolution increases the network traffic that can result the packet loss over the network. The criticality of the situation is increased when the network is also suffering from some attack or the heavy load over the network that performs the flooding so that that the networks delay is increased over the network. In this paper, a distinctive multipath based data chunk sequencing scheme is suggested to perform the reliable communication over the clustered mobile network.

Keywords: MANET, video transmission, optimized route generation.

I. INTRODUCTION

Mobile Ad-hoc network are self-configuring infrastructure less network of mobile devices connected by wireless. Since the network is decentralized, where all network activity including discovering the topology, delivering messages must be executed by the nodes themselves. As MANET network are infrastructure less there exist no dedicated routers. Instead, all mobile nodes act as a router and also responsible for discovering and maintaining routes. Furthermore without centralized administration, MANETs can be called autonomous. MANETs suffer from temporary link failures and route changes. A Mobile network is a hybrid network on which the different kind of data is communicated. MULTIMEDIA data transmission experience a number of constrains that result to low Quality of Service (QoS) that is offered to the end user. These constrains have mainly to do with the nature of multimedia applications, which are characterized by three main properties: the demand for high data transmission rate (bandwidth-consuming

applications), the sensitiveness to packet delays (latency and jitter) and the tolerance to packet losses (packet-loss tolerant applications), when compared to other kind of applications. Video streaming in MANETs [1] is one of the most challenging issues. Video streaming in MANETs is mainly affected by these factors like node mobility, dynamic change in topology, multi path shadowing and fading, collusion, interference and many more. The dynamic change in topology causes periodic connectivity which results in large packet loss. Packet loss has the largest impact on the quality of the video. Video streaming in real time requires special techniques that can overcome the losses of packets in the unreliable networks [2]. Video has been an important media for communications and entertainment for many decades. The growth and popularity of the Internet in the mid-1990s motivated video communication over best effort packet networks. Video over best effort packet networks is complicated by a number of factors including unknown and time-varying bandwidth, delay, and losses, as well as many additional issues such as how to fairly share the network resources amongst many flows and how to efficiently perform one-to-many communication for popular content. Video communication over a dynamic environment, such as a mobile and wireless network is much more difficult than over a static channel, since the bandwidth, delay, and loss are not known in advance and are unbounded. Types of Multimedia streaming application:- there are various types of multimedia application as follow :

A. Streaming stored multimedia

Multimedia content is stored at the server, a user may request for a file at any time. There are two modes for transmission of stored multimedia over the Internet, namely the download mode and the streaming mode. In the download mode, a user downloads the entire audio or video file and then plays back file. However, full file transfer in the download mode usually suffers long and perhaps unacceptable transfer time. In contrast, in the streaming mode, the multimedia content need not be downloaded in full, but is being played out while parts of the content are being received and decoded. In this mode,

user may perform simple operation like pause, resume, forward e.g. Video on Demand, Online Music etc.

B. One to many streaming of real-time multimedia

It is very similar to traditional radio and TV broadcast but in this transmission takes place over the internet. Typically, there are many users who are simultaneously receiving the same real-time audio/video program. This type of applications is non-interactive i.e. a client cannot stop or forward the media while playing. Video data in live streaming is generated at the same time of transmission. Only initial delay up to 10 seconds can be tolerated. E.g. Live TV streaming, online radio etc

C. Real-time interactive multimedia

In this type of streaming, users can use audio/video to communicate with each other in real time e.g. internet phone, video conferencing, interactive games etc. The delay should be less than a few hundred milliseconds. For voice, delays smaller than 150 milliseconds are not perceived by a human listener, delays between 150 and 400 milliseconds can be acceptable, and delays exceeding 400 milliseconds result frustrating voice conversations. Due to this real time constraint, it is very difficult to handle and implement.

The paper is organized as follows. Section II of this paper includes the related work done by various authors in this field. In section III novelty of proposed idea is given. Section IV includes the proposed technique in detail. Experiment design for the simulation is present in section V. The work is concluded in section VI with a finding that DMBDCSS performs better for those network transmitting multimedia data.

II. RELATED WORK

According to [3], 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 [4], 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 [5-7] 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 [7] 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 [8] 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. [8] 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. NOVELITY OF PROPOSED TECHNIQUE

Video streaming in MANETs [1] is one of the most challenging issues. Video streaming in MANETs is mainly affected by these factors like node mobility, dynamic change in topology, multi path shadowing and fading, collusion, interference and many more. The dynamic change in topology causes periodic connectivity which results in large packet loss. Packet loss has the largest impact on the quality of the video. Video streaming in real time requires special techniques that can overcome the losses of packets in the unreliable networks [2].The presented technique uses distinctive path scheme so that the load over a specific node is not increased that helps in reducing data loss. It also identifies the effective route based on communication analysis so that the attack preventive communication can be performed. The parallel communication over the network improves the effectiveness of communication.

IV. DISTINCTIVE MULTIPATH BASED DATA CHUNK SEQUENCING SCHEME

One of the critical communicating data type over network is video transmission. Video Transmission with high resolution increases the network traffic that can result in 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 the effective communication over this delayed mobile network, a distinctive multipath based data chunk sequencing scheme is explained in this section. The presented approach is divided in three main stages. In first stage, the optimized route between the source and destination is identified. The route identification is done under different parameters. The parameters included are loss analysis and delay 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 do not share any common intermediate node. In this stage, the attacker node identification is done at the initial stage, the node having the delay more than threshold value is treated as

the attacker node or the delay node. After this stage, N numbers of attack preventive routes are identified. Now to start the actual communication, in third stage, the video data is converted to small chunks. The data chunks are identified based on the available routes so that each route gets M data chunks. Finally, these data chunks are sent in parallel on multiple paths so that the network traffic is distributed. At the receiver end, the data is accepted from all these chunks and retrieved as the final video data.

PROPOSED ALGORITHM (DMBDCSS)

There are following main steps that this algorithm performs:

- Generate distance matrix.
- Identify min. hop distance
- Generate the Average Energy specification on neighbor node list.
- Identify Minimum Distance and High Energy Node from Enable Neighbor List called Node

Algotithm:

{
1. Setup a Mobile Network with N Node Specification with Energy Constraint
2. Define Source Node Src and Destination Node Dst
3. Generate the DistancePath over the network called DistMat
4. While (Src<>Dst)
[Repeat Process till Destination Node not arrive]
{
5. Identify the NeighborNodes for Src called NeighList
6. [MinDist Index]=MinDistance(NeighList)
[Identify the Minimum Distance Hop]
7. MaxE=MaxEnergy(NeighList)
MinE=MinEnergy(NeighList)
Avg=(MaxE+MinE)/2
[Generate the Average Energy specification on neighbor node list]
8. For j=1 to length(NeighList)
[Process All Neighbors]
{
9. if (Energy(Node(j)<Avg)
{
Nodes(j).Status=Disable
}}
10. Identify Minimum Distance and High Energy Node from Enable Neighbor List called Node K
11. Set NextHop=Nodes(K)
[Identify Next Effective Next Hop]
}}

For simulating the network, we have taken 10 nodes with node 0 being source node and node 9 being destination node. Communication is started on optimized route between node 0 and node 9. Following figue 1(a) shows when energy of nodes reaches critical level, nodes with low energy will turn yellow indicating critical energy level. And finally when their energy becomes less than average energy, these nodes will turn red and such nodes become disabled nodes as shown in figure 1(b).

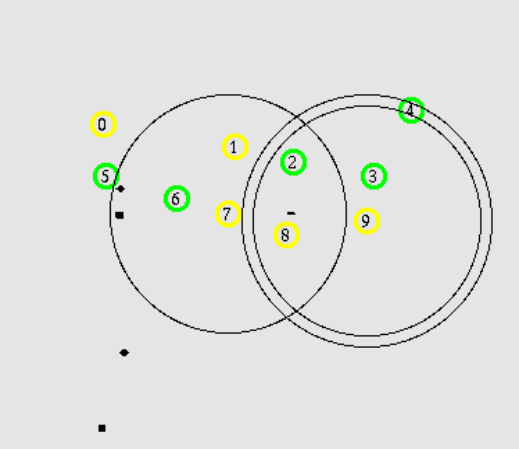

Fig1(a). Nodes when reaches critical energy level

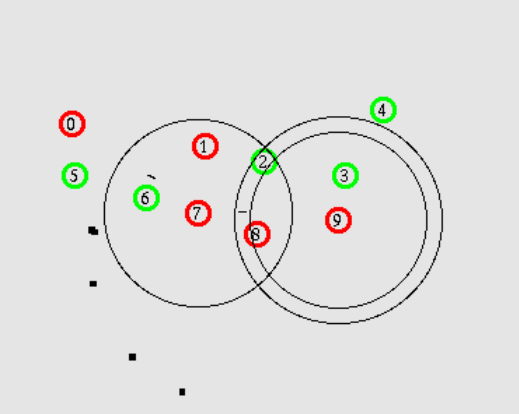

Fig1(b). Nodes when reaches below average energy

Results obtained from suggested algorithm are discussed in following section.

V. RESULTS

To calculate the impact of the proposed algorithm, simulation of MANET is done using NS2(Network Simulator). The simulation scenario consists of 10 nodes with source node being 0 and destination node being 9. Simulation is shown in figure 1 above. Common parameters used are listed in table1.

PARAMETER	VALUE

Platform	UBUNTU
Simulator	NS2
Network Size	10 Nodes
Traffic Type	Video
Address Mode	IPV4
Ad Hoc Routing Protocol	AODV
AODV Parameters	Default

Table1. Common parameters

Figure 2(a) shows no. of packets transmitted over time using our proposed approach and using an existing approach(normal transmission). It clearly indicates more no. of packets transmission in case of our proposed approach which means increased throughput in case of proposed approach.

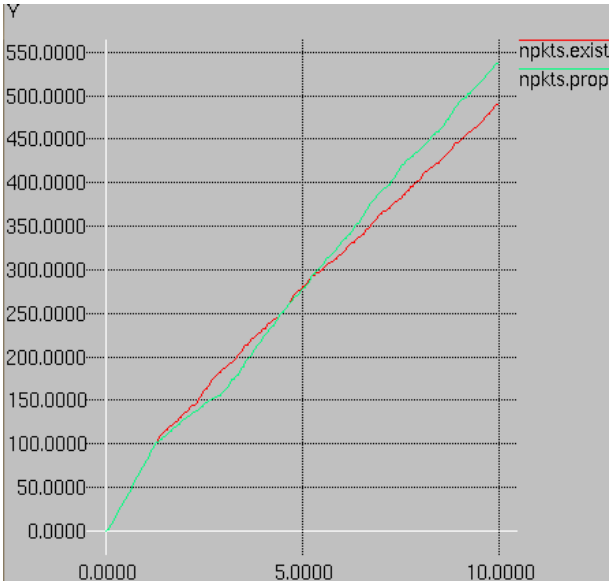

Fig2(a). Packets transmitted

Figure 2(b) shows comparative result of packets lost over time using proposed and existing approaches. It indicates gradual decrease in no. of packets lost in case of proposed approach i.e., low lost rate is achieved which means better quality transmission is performed using our effective approach. Similarly figure 2(c) shows low delay is achieved using DMBDCSS approach.

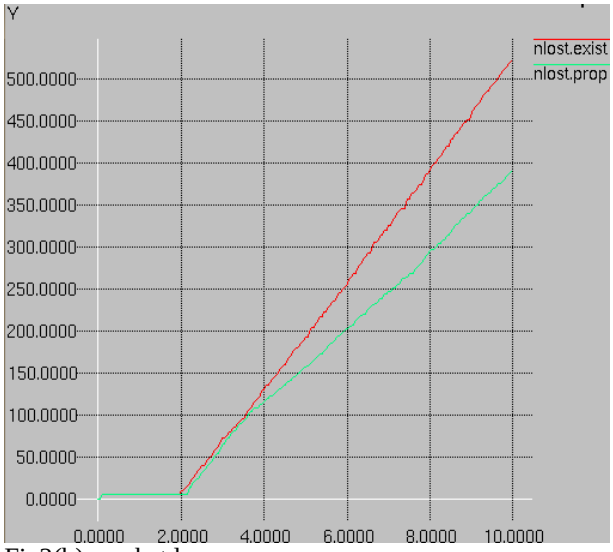

Fig2(b). packet loss

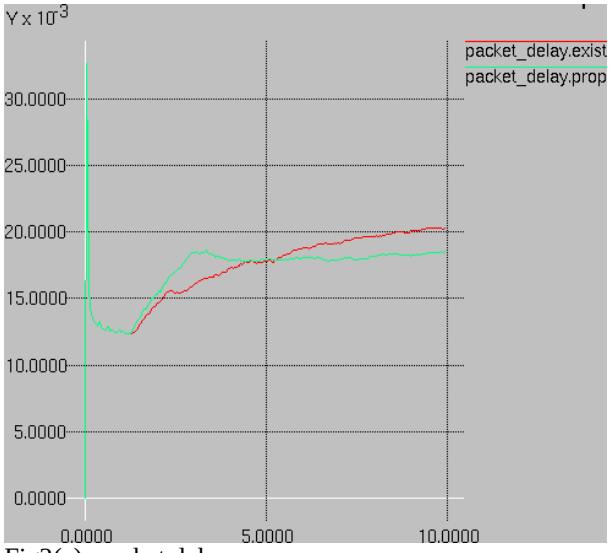

Fig2(c). packet delay

VI. CONCLUSION

In this paper we have suggested an attack preventing routing scheme that is implemented in ns2. To provide an effective communication over this delayed mobile network, this distinctive multipath based data chunk sequencing scheme is suggested. Proposed technique is very effective to detect and prevent the Dropping Attack. As this technique uses the distinctive path scheme so load over a specific node is not increased that reduces the data loss. Packet delivery ratio and throughput are greatly enhanced using suggested effective (DMBDCSS) approach.

VII. REFERENCES

[1] Harsharndeep Singh,Meenu Dhiman, Pankaj Kumar Sehgal ―A Survey on Video Streaming Schemes over. MANETs‖ Vol. 2, Issue 3, May-Jun 2012, pp.1116-1122.

[2] Tim Bohrloch,Carlos T. Calafate, A. Torres, J.C.Cano, P.Manzoni, ―Evaluating video streaming performance in MANETs using a testbed,‖ XXII Jornadas de Paralelismo Sept.2011.

[3] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. IEEE Security and Privacy, 2(3):28–39, 2004.
[4] 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.
[5] 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.
[6] 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.
[7] T. Yuksel, "Partial Encryption of Video for Communication and Storage" Master's Thesis, The Middle East Technical University, pp. 1-2, September 2003
[8] 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.
[9] 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
[10] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. Rtp: A transport protocol for real-time applications, Internet RFC 3550, 2003.