ANALYSIS OF DYNAMIC HOP-AWARE BUFFER MANAGEMENT SCHEME FOR MANET.

Dr.R.MANIKANDAN , Assistant Professor , Computer Science and Engineering , Government College of Engineering,Dharmapuri. **rmkmanikandan@yahoo.co.uk**

R.SUDHAN and K.VINOTH , Computer Science and Engineering , Government College of Engineering,Dharmapuri. **sudhanmax1995@gmail.com , vinoovijay5353@gmail.com**

ABSTRACT

The wireless ad hoc network, the mobile ad hoc network is one of the most popular network technologies in research and development. The network's ad-hoc nature kept attracting researchers and engineers to find new and improved techniques. This article presents an analysis of ad hoc network and buffer management technology for mobile devices. We propose a dynamic Hop Aware Buffering (DHAB) scheme to reduce packet losses and delays in MANETs. In this scheme, the buffer is virtually partitioned based on the number of hops passed and the significance of the packet. This article examines resource depletion attacks on the AODV protocol layer, which disable networks by rapidly degrading the node's battery power. These vampire attacks are not specific to a particular protocol, but depend on the characteristics of many known protocol classes. We find that all the logs under investigation are affected by vampire attacks that are destroyed, difficult to detect, and easy to execute if only a malicious insider sends only protocol-compliant messages. In the worst case, a single vampire can increase network-wide power consumption by a factor of O (N), where N equals the number of network nodes. The methods we discuss to mitigate these types of attacks include a new proof-of-concept protocol that limits the damage caused by vampires during packet forwarding. In addition, the size of the virtual partitions changes dynamically depending on the usage and security threshold of the partition.

Keywords: *Mobile ad hoc Network, Buffer Management Technique, Dynamic Hop Aware Buffering, Back-tracking Algorithm, Vampire attacks.*

1. INTRODUCTION

The demand for speed in wireless networks is constantly increasing. More recently, cooperative wireless communication has received tremendous interest as an untapped means of improving the performance of information transfer operating across the ever-challenging wireless medium. Cooperative communication has emerged as a new dimension of diversity to emulate the strategies developed

for multiple antenna systems because a wireless mobile device may not be able to support multiple transmit antennas due to size, cost, or hardware limitations. By exploiting the broadcast nature of the wireless channel, the cooperative communication allows antennas with a single antenna to share their antennas to form a virtual antenna array and provides significant performance improvements. This promising technology was considered in the IEEE 802.16j standard and is expected to be integrated into 3GPP Long Term Evolution (LTE) multi-hop mobile networks.

An extension of wireless LAN operating in ad hoc mode is multi-hop ad hoc networks. They are typically used in large areas. A wireless multi-hop ad hoc network is a network of nodes (e.g., computers, mobile nodes, etc.) connected by wireless communication links. The connections are usually implemented with digital packet radio equipment. The transmission range of the radio is very limited. Some devices may not be able to communicate directly with one another due to their limited wireless range. These networks need different intermediate nodes to forward messages. In such cases, intermediate devices act as relays.

The effect of Vampire attacks are consider on link-state, distance vector, source routing and beacon routing protocols also a logical ID-based sensor network routing protocol. According to above stated protocols we view the covered protocols as an important subset of the routing solution that our attacks are likely to apply to other protocols. All routing protocols employ at least one topology discovery period. Our attackers are malicious insiders having the same resources and level of network access as honest nodes. Attacker location within the network is assumed to be fixed and random. This is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks.

The cache allocates all neighboring nodes in proportion to the number of packets received from neighbors. However, there is no difference between the long and the short hop packets. The Hop Aware Buffering (HAB) Scheme is designed specifically for wireless ad hoc networks. However, the importance of the packets (i.e., real-time or non-real-time packets) has not been considered. Another disadvantage of HAB is that duty planning is assumed to be random. The work overcomes the lack of HAB. The dynamics of the buffer was not discussed. The contribution of this paper is twofold. First, we suggest a dynamic Hop Aware Buffering (DHAB) scheme that splits the buffer space into four partitions based on the number of hops along with the QoS of the packets. Second, the size of each partition changes dynamically according to the traffic load and security thresholds of the partition.

2. RELETED WORK

2.1 Adaptive red: an algorithm for increasing the robustness of red active queue management

S. Floyd, R. Gummadi, and S. Shenker was said the End-to-end congestion control is widely used in the current Internet to prevent congestion collapse. However, because data traffic is inherently bursty, routers are provisioned with fairly large buffers to absorb this burstiness and maintain high link utilization. The downside of these large buffers is that if traditional drop-tail buffer management is used, there will be high queuing delays at congested routers. Thus, drop-tail buffer management forces network operators to choose between high utilization (requiring large buffers), or low delay (requiring small buffers). Delay being a major component of the quality of service delivered to their customers, network operators would naturally like to have a rough a priori estimate of the average delays in their congested routers; to achieve such predictable average delays with RED would require constant tuning of the parameters to adjust to current traffic conditions. Our goal in this paper is to solve this problem with minimal changes to the overall RED algorithm. To do so, we revisit the Adaptive RED proposal of Feng et al. from 1997 [6, 7]. We make several algorithmic modifications to this proposal, while leaving the basic idea intact, and then evaluate its performance using simulation. We find that this revised version of Adaptive RED, which can be implemented as a simple extension within RED routers, removes the sensitivity to parameters that affect RED's performance and can reliably achieve a specified target average queue length in a wide variety of traffic scenarios. Based on extensive simulations, we believe that Adaptive RED is sufficiently robust for deployment in routers.

2.2 Buffer Occupancy of Double-Buffer Traffic Shaper in Real-Time Multimedia Applications across Slow-Speed Links

A. O. Oluwatope, D. T. Oyewo, F. E. Olayiwola, G. A. Aderounmu and E. A. Adagunodo was said the concept for In this paper, a double-buffer traffic shaper was investigated to adjust video frame rate inflow into theTCP sender-buffer of a multimedia application source across a slow-speed link. In order to guarantee QoS across a slow-speed link (*i.e.* < 1 MBPS), the double-buffer traffic shaper was developed. In this paper, the buffer size dynamics of double-buffer was investigated. The arrival and departure of frames were modeled as a stochastic process. The transition matrix for the process was generated and the stationary probability computed. A simulation program was written in Matlab 7.0 to monitor the buffer fullness of the second buffer when a 3600 seconds H.263 encoder trace data was used as test data. In the second buffer, it was discovered that over 90% of the play-time, the buffer occupancy was upper bounded at 300 frames per second and utilization maintained below 30%.

2.3 Competitive buffer management with packet dependencies

A. Kesselman, B. Patt-Shamir and G. Scalosub was says the Specifically, we consider

the following scenario. There is a FIFO buffer which can hold B packets. The packets arrive at the buffer according to an adversarial process, but only one packet can be sent out of the buffer in each time step. Therefore, overflows may occur, and the buffer management algorithm tries to minimize their damage. The new variant we consider here models dependencies among the arriving packets. In particular, we consider the common case where the arriving data stream originally consists of large frames, while the data link can carry only small packets, and therefore each frame must be fragmented into a few packets. This scenario introduces dependencies, because, for example, in many cases a frame is useless unless all its constituent packets are delivered. It follows that in this common case, deciding which packet to drop may influence the decision about packets that may arrive only in the distant future, giving rise to new algorithmic questions. For example, it turns out that some natural algorithms perform very poorly in the context of packets with dependencies, whereas other algorithms work relatively well.

Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one.

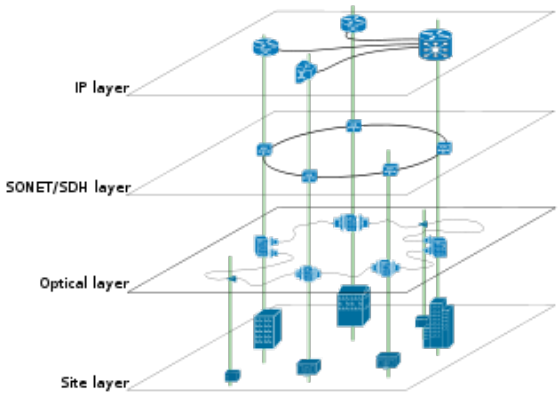

Fig 2.1: A sample overlay network: IP over SONET over Optical

For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network .

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of sub networks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully-connected IP overlay network to the underlying ones.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. On the other hand, an overlay network can be incrementally

deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

Network security

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network Security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network Security is involved in organization, enterprises, and all other type of institutions. It does as its titles explains, secures the network. Protects and oversees operations being done.

3. PROPOSED SYSTEM

We propose an advanced protocol for control scheme to develop network connectivity in MANETs by jointly considering both the upper layer network capacity and the physical layer cooperative communication. We propose a dynamic Hop Aware Buffering (DHAB) scheme to reduce packet loss and delay in MANETs by testing the performance of the proposed backtracking algorithms for various variable orders, order of values, and consistency enforcement. This paper also recognizes the particular node acting as a vampire node causing large routes or loops in the network and also eliminating this vampire node to prevent forwarding of packets from the source-destination route. In this article, we discuss the effects of vampire attacks on ad hoc on-demand vector routing (AODV). It can be observed that the variable and value order of backtracking with consistency enforcement techniques provides better results. In the work, the backtracking-based method focused primarily on avoiding vampire attacks in the discovery phase of DHAB by checking the signal strength of the nodes sending the group connecting messages. A vampire would send a high energy signal to suppress the group linking messages from another node. So avoid a node that sends with high signal strength.

4. DYNAMIC HOP-AWARE BUFFERING (DHAB) SCHEME

The structure of the DHAB is divided into four components: the classifier, the queue size

manager, the partitioned buffer, and the scheduler. The following sections describe DHAB components in detail.

4.1 Classifier

The classifier is responsible for distinguishing packets based on the following criteria: 1) type of packets (i.e., real-time packet such as VoIP and multimedia audio / video or non-real-time packet such as text file). This information can be easily obtained from the packet header. 2) Number of hops M that traversed the packet from its source and to an intermediate node that can be easily obtained from the routing table information.

4.2 Queue Manager

The size of each partition can be changed dynamically according to the traffic load of each class. This is the main function of the Queue Manager (QM). The QM manages the VPs of the buffer using Borrow and Push-Out strategies. The borrowing strategy moves the free space from one VP with Maximum Free Space (MFS) to another. It is important to note that borrowing can only be done if there is unused space in the buffer. The push-out strategy discards packets when there is no more room in all VPs. To achieve this goal, we have defined the thresholds T1 and T2 to receptively secure the VPs of LHRT and SHRT. In addition, we define the threshold T as protection for both LHNRT and SHNRT. Regarding the values of the thresholds, DHAB pushes packets from one VP and the generation space exits to another VP.

4.3 Buffer Management Evaluation

Problems in the Buffer Management Scheme There are several variables introduced in the QoS paradigm regarding queues, but this quadratic measure is managed by the process. In addition, the buffer size plays a crucial role in the diversity of packets that are command-strong is before dropping the fresh packet (an arrived case of the buffer overflow) Drop Tail's Queue Management theme has been used for several years, during which packets were fully populated once quadratic ally. The length of the buffer is the buffer so most of the parameter controls the package that come from this topic. Later, Active Queue Management (AQM) was introduced, which is currently prevalent in the world. While this is the causative node, subject is previously complaining, so the queue is only the sender will cease to cause less knowledge or speed of information transfer. In the meantime, this length of the queue is shortened with the process and the reordering of buffered packets. Once a decent area is back on the market within the supply, the queue may send additional packets to the query.

BACKTRACKING ALGOIRITHM

1. Routing Protocol: AODV
2. Source node S starts route discovery to locate Destination node D.

3. Source node S broadcasts RREQs packet to its neighbors after adding “flag” field & initializing its value to 0.
4. If (neighbor node = = destination node) { Destination node D accepts RREQs and
Send RREP to Source node S.
Return.
}
5. If (Whether RREQ contains its own ID == true) {
1. Intermediate node will return a RREQ packet to source node S by updating a value of “flag” field to 1.
2. Source node S will send the entire list of appended node IDs in RREQ to centralized entity (CE) and try to find another route except this route.
3. CE will store all routes along with all appended node IDs submitted by various source nodes.
4. If (If no. of routes < 3 in CE) {
Go to Step 5.3 (within if case).
}
5. Centralized Entity (CE) finds common list of nodes from those routes which causes vampire attack.
$X = R_i \cap R_j \cap R_k$ where i, j & k are three different routes in set i j k CE.
6. Centralized Entity (CE) broadcast common list of nodes X within entire network in order to ignore set them.
7. Return
}
Else {
1. Intermediate node will append its own ID in RREQ packet & forward it to its neighbor.
2. Go to s
}}

5. EXPERIMENTAL RESULTS

To test the proposed DHAB scheme, a discrete event simulator was developed using the network simulation tool platform. We assumed that all nodes have real-time and non-real-time to transmit the entire simulation time, and the channel transfer is not free. The values of the simulation operating parameters are listed in detail in Table I. The maintenance time is determined by the channel loss rate 1-.alpha. caused and controlled by the threshold T. The service priority is given to the real-time packets over the non-real-time packets and can be increased or decreased based on the status of the traffic load. For the sake of fairness between the four classes, the optimal value of the channel loss rate 1-α is estimated by the simulation.

In this type of attack, a series of loops is formed between the source and the sink node. Therefore, the route length is increased and exceeds the limit of the nodes in the network. This increases the power consumption of nodes and thus minimizes network lifetime. With a factor of O (λ) the energy consumption increases, whereby the maximum distance λ is. The energy consumption during the attack is measured.

The stretch attack is performed on wireless sensor networks, shown in Figure 3. This type of attack artificially creates a long path from source to sink through an enemy, causing packets to cross a larger route and drain additional energy. This attack causes a node that is not on the optimal path to process packets. By a factor of O (min (N, λ)), where the number of nodes in the network is N and the maximum path length is λ. The energy consumption during the attack is measured.

Vampires have less control over the packet when the packet is independently routed, but malicious nodes can route the packet to any part of the network called a Directional Antenna Attack. Malicious discovery attack: Send sender discovery packet, malicious nodes also send discovery packet on the network. The nodes that hear the recognition message send a reply to the sender nodes, but because some recognition messages are malicious, the response to these messages may not arrive at the destination due to malicious nodes that are not found. This leads to a loss of energy in the network.

In this scenario, there are four sources S1, S2, S3, and S4 that simultaneously send LHRT, LHNRT, SHRT, and SHNRT packets to the same destination D. There are three relay nodes R1, R2 and R3. The relay node R3 is a common relay for all sources. Usually, packages with fewer relays (ie, from S3 and S4) have the advantage of occupying most of the buffer space in R3. However, based on DHAB, the buffer of relay node R3 classifies and buffers the packets according to the number of hops and their importance. Therefore, DHAB aims to reduce transmission losses and delays.

TABLE I: List of the simulation operational parameters

Parameter	Value
The total buffer size B	100 pkts
The virtual buffer size of each class	$\lfloor \frac{100}{4} \rfloor$ pkts
LHRT safe area threshold T_1	30, 60 pkts
SHRT safe area threshold T_2	20, 30 pkts
The service threshold T	20 pkts
Transmission range	50 m
Packet size	2048 bytes
Routing protocol	$AODV$
Simulation time	10^6 $Millisecond$
The traffic load	varies

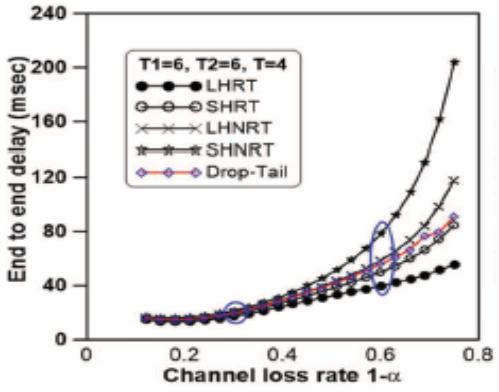

Fig 5.1: Channel loss rate against the end to end delay

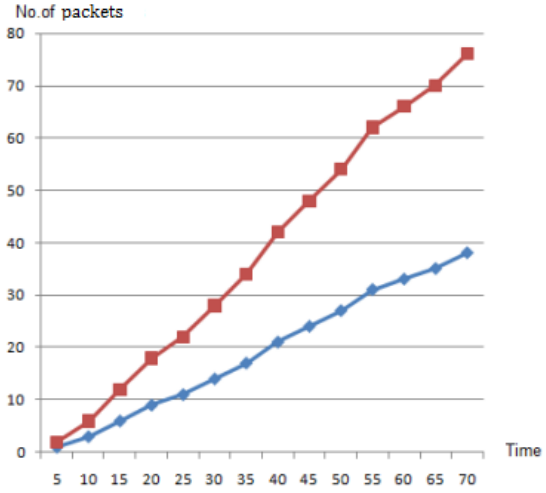

Fig 5.2: simulated results of Packet loss based on traffic

From Figure 5.1, we note that the best value of $1 - \alpha$ is $0.1 \leq 1 - \alpha \leq 0.4$ where the end-to-end delays of DHAB and Drop Tail close to each other. Figure 5.2 illustrates that vampire attacks are identified in discovery phase also. So chances of composition and transmission of unwanted data packets are reduced, if a node is identified as vampire node.

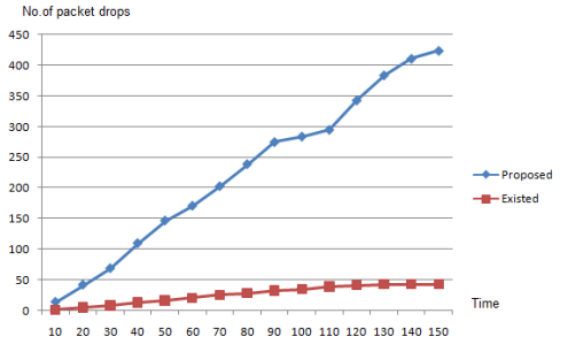

Fig 5.3: Throughput

6. CONCLUSION

In MANETs, packet loss and end-to-end delay are two important parameters for evaluating the performance of these networks. The type of buffer management scheme at the intermediate nodes plays an essential role in increasing or decreasing these parameters. The proposed DHAB scheme takes into account these unique properties of such networks. The dynamically settable buffer gives the nodes using DHAB the advantages of reducing the likelihood of loss and end-to-end delay. The analysis and simulation results show that the DHAB surpasses the drop-tail scheme and the QoS of the various types of traffic can be easily controlled by careful selection of thresholds T, T1 and T2. The results also show that the variable and value ordering have strong effect on the exploration of solutions in backtracking approach.. However, the task-oriented solution representation is observed to give solutions in lesser time. Also, the outcome of the proposed consistency enforcement approach shows significant increasing throughput and packet loss in time required to obtain solutions.

REFERENCES

[1] S. Floyd, R. Gummadi, and S. Shenker, "Adaptive red: an algorithm for increasing the robustness of red active queue management," Technical report, International Computer Science Institute (ICSI), Berkeley, California, 2001.

[2] A. O. Oluwatope, D. T. Oyewo, F. E. Olayiwola, G. A. Aderounmu and E. A. Adagunodo, "Buffer Occupancy of Double-Buffer Traffic Shaper in Real-Time Multimedia Applications across Slow-Speed Links", CN, vol. 05, no. 01, pp. 84-92, 2013.

[3] A. Kesselman, B. Patt-Shamir and G. Scalosub, "Competitive buffer management with packet dependencies", 2009 IEEE International Symposium on Parallel & Distributed Processing, 2009.

[4] M. Aamir and M. Zaidi, "A buffer management scheme for packet queues in

MANET", Tinshhua Sci. Technol., vol. 18, no. 6, pp. 543-553, 2013.

[5] M. Kalil, H. Al-Mahdi and A. Mitschele-Thiel, "Performance Evaluation of Hop-Aware Buffer Management Scheme in Multihop Ad Hoc Networks", 2008 The Fourth International Conference on Wireless and Mobile Communications, 2008.

[6] W. Lai, M. Weng and Y. Lin, "Improving MANET performance by a hop-aware and energy-based buffer management scheme", Wireless Communications and Mobile Computing, Wiley, vol. 14, no. 7, pp. 704- 716, 2014.

[7] Bisnik, Nabhendra, and Alhussein A. Abouzeid. "Queuing network models for delay analysis of multihop wireless ad hoc networks." Ad Hoc Networks 7.1 (2009): 79-97.âA˘ R

[8] Pavan Pichka, H Santhi, N Jaisankar, S Devi Priya, "A Comprehensive Study of Existing Multicast Routing Protocols Used In Mobile Ad Hoc Networks", *International Journal of Engineering Science and Technology (IJEST)*, vol. 4, no. 05, May 2012.

[9] Tanu Preet Singh, Neha, Vikrant Das, "Multicast routing Protocols In MANETS", *International journal of Advanced Research in Computer Science and software Engineering*, vol. 2, no. 1, January 2012.

[10] S Aruna, A Vanitha, A Subramani, "Performance Analysis of Ad hoc routing protocols im multicast enviornment", *Journal of Computer Applications (JCA)*, vol. IV, no. 2, 2011, ISSN 0974-1925.