Available online at www.elixirpublishers.com (Elixir International Journal)

Adoc Network

Elixir Adoc Network 59 (2013) 15781-15785

ISSN: 2229-712X

Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks

K.Priya[1,*], Ujwal A. Lanjewar[2], K.Prasuna[3] and Chilakalapudi Meher Babu[4]
[1]P. B. Siddhartha College of Arts and Science, Vijayawada (A.P), India.
[2]Faculty of Computer Science, R.T.M. Nagpur University, Nagpur.
[3]ECE Department, Vijaya Institute of Technology for Women, Vijayawada (A.P.), India.
[4]Department of Computer Science & Engineering, NIST, Vijayawada (A.P), India.

ARTICLE INFO

Article history:
Received: 23 April 2013;
Received in revised form:
10 June 2013;
Accepted: 14 June 2013;

Keywords
Mobile Adhoc network Architecture,
Cognitive radio,
Ad hoc networks,
Cross Layer Design,
Common control.

ABSTRACT

Multi-hop Wireless Networks (MHWNs) are anticipated to play an important role at the edge of the Internet, enabling a large number of innovative applications. The great demand for capacity from a large number of users and applications, coupled with the sparse bandwidth available on the wireless channel, place particular emphasis on effective congestion management approaches. Effective and well-studied algorithms for congestion control at the transport layer exist in wired networks. However, for a number of reasons, these approaches do not translate directly to wireless environments. In this chapter, we first describe the problem of congestion control in MHWNs, and discuss approaches for solving it. The presentation is organized into two components: (1) a review of the causes of congestion and algorithms for congestion avoidance in MHWNs at different layers of protocol stack; and (2) a review of analytical models for the rate control problem and their use for congestion control.

1. Introduction

Congestion avoidance mechanisms can be broadly divided into detection and control. Congestion can be detected by monitoring the queuing delays and packet drops at the nodes. Congestion control is generally achieved by regulating the packet-sending rate at the source node of the connection. The source node infers the congestion information along the connection route for effective congestion control. To enable the source node to control packet-sending rate, the intermediate routers proactively send the observed congestion levels to the participating sources. In such proactive schemes, the routers detect congestion by monitoring the queuing delays and packet drops at intermediate routers and send the required information to the source nodes. Another alternative is a passive mechanism where the source node infers the congestion level by measuring parameters like end-to-end packet delays. A hybrid of active and passive approach is used in the Internet. In a wired network, the packet drop information accurately conveys the congestion information since packet drops are primarily due overflow of queues at intermediate nodes. Packet drops due to channel error or ineffective MAC protocol is very rare. The end-to-end packet delays are primarily due to the intermediate queuing delays since the transmission time is low.

For example, packet drops can be caused due to a high channel error rate. The end-to-end delays can be skewed due to the wireless MAC layer transmission scheme, which can significantly increase the transmission time of a packet.

2. Nature of Cross Layer Design

TCP is a reliable connection-oriented byte-stream protocol which performs congestion control dynamically during the data communication process. TCP congestion control is performed on an end-to-end basis.

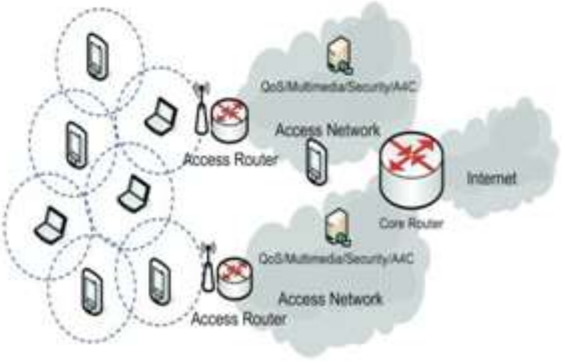

Fig. 1. Example of a simple ad-hoc with connecting nodes

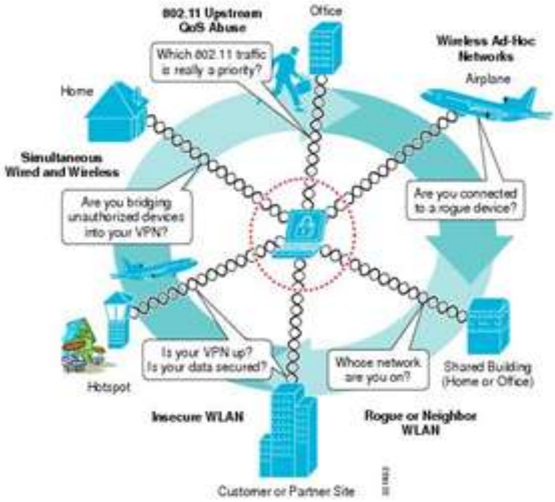
802.11 Upstream QoS Abuse
Office
Which 802.11 traffic is really a priority?
Wireless Ad-Hoc Networks
Airplane
Home
Simultaneous Wired and Wireless
Are you bridging unauthorized devices into your VPN?
Are you connected to a rogue device?
Is your VPN up? Is your data secured?
Whose network are you on?
Shared Building (Home or Office)
Hotspot
Insecure WLAN
Rogue or Neighbor WLAN
Customer or Partner Site

Fig. 2 Traffic of connecting nodes

Tele:
E-mail addresses: pppriyamca@gmail.com

The receiver provides an acknowledgement (ACK) feedback back to the sender. Relying on the information provided by ACKs, the sender can detect which packets are lost during transmission over the communication path.

TCP uses additive increase and multiplicative decrease strategy for its window adjustment according to network conditions. The connection is initiated with window size equal to one packet (1 MSS—Maximum Segment Size). Then, cwnd is increased exponentially for every non-duplicate ACK reception until the Slow Start Threshold (ssthresh) is reached. Prior the connection establishment, ssthresh is set to an initial value, which depends on the implementation of the protocol stack, and then adjusted on the basis of the estimate of the network capacity. This technique is called slow start phase.

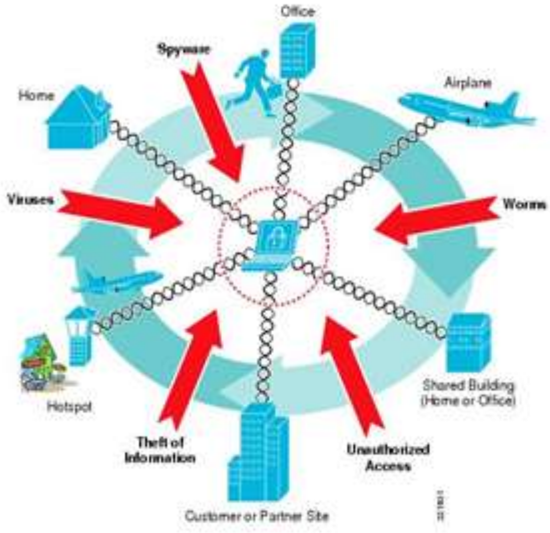

Fig. 3. Example Congestion of connecting nodes

When the threshold is reached, TCP enters congestion avoidance phase. The window is increased linearly by one packet for each received ACK. The window growth in this phase is limited to a maximum window size, negotiated between sender and receiver during connection establishment and then updated on the fly during the communication process (the receivers advertised window). There are two ways for TCP sender to detect data loss occurred on the communication link: reception of duplicate ACKs (dupacks) and timeout occurrence. In the first case, a dupack is generated by the receiver upon reception of an out-of-order.

3. Research challenges

3.1.1 Band Sensing

One of the primary requirements of Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks is their ability to scan the band and identify vacant channels available for opportunistic transmission. As the primary user network is physically separate from the secondary user network, the secondary users do not get any direct feedback from primary users regarding their transmission. The secondary users have to depend on their own individual or cooperative sensing ability to detect primary user transmissions. Since the primary users can be spread across a huge geographical area, sensing the entire spectral band accurately is a challenging task. The secondary users have to rely on weak primary transmission signals to estimate their presence.

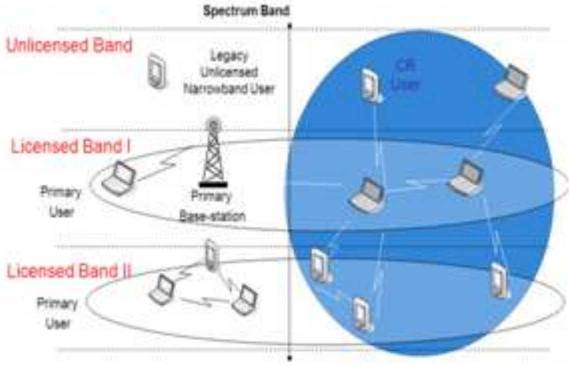

Fig. 4. Band sensing of connecting nodes

Most of the research on Band-sensing techniques falls Security Issues in Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks into three categories: transmitter detection, cooperative detection and interference-based detection. The main aim of all these techniques is to avoid interference to primary transmissions. The amount of interference caused by all the secondary users at a point in space is referred to as the interference temperature at that point. When a primary user transmission is taking place, the interference temperature should be below a specified threshold near the primary receivers.

3.1.2 Band Analysis and Decision

Band sensing determines a list of available bands. In addition to that can be used to evaluate their effectiveness are interference of path loss, wireless link errors, link layer delay and holding time (expected duration that the secondary user can occupy the band).

3*.1.3 Band Mobility*

Band mobility refers to the agility of Cross Layer in Wireless Mobile AD-HOC Networks to dynamically switch between Band accesses. One of the primary factors affecting Band mobility is the delay incurred during Band handoff. This delay adversely affects protocols employed at various layers of the communication protocol stack.

3.2.1 Centralized Congestion Control Networks

These base stations control the medium access and the secondary users. The secondary users are synchronized with their base stations and may perform periodic Band-sensing operations.

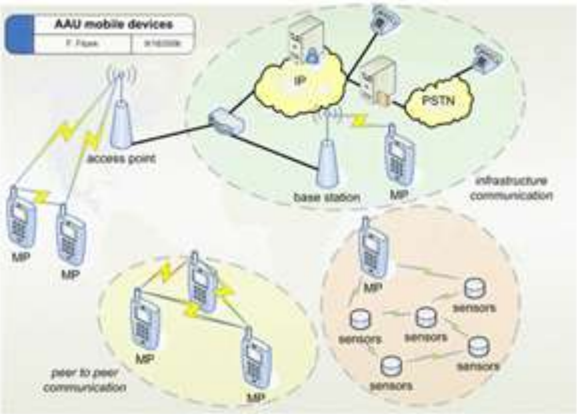

Fig. 5. Band Analysis of connecting nodes

The secondary base stations can be interconnected through a wired backbone network.

3.2.2 Decentralized Congestion Control Networks

In a decentralized architecture, the secondary users are not interconnected by an Infrastructure-oriented network represents a decentralized network, where Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks Secondary user Primary user Secondary base station Primary base station.

3.3.1. Attacks on Congestion Control Networks

Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks as any activity that results in (a) unacceptable interference to the licensed primary users or (b) missed opportunities for secondary users. An attack is considered strong if it involves a minimal number of adversaries performing minimal operations but causing maximum damage/loss to the primary and or secondary users in the network. We describe attacks on five layers in the protocol stack, namely, the physical layer, link layer, network layer, transport layer and application layer.

3.3.2. Physical Layer Attacks

The physical layer is the most basic layer in the protocol stack. It provides the means of transmitting raw signals over the transmission medium. The physical layer determines the bit rate, channel capacity, bandwidth and maximum throughput of the connection. In Congestion Control networks, the physical layer has the capability to transmit at various frequencies across most of the Band. Therefore, when transmission from one frequency band is switched to another frequency band, the switching process **Attacks** on Congestion Control Networks incurs considerable delay in the physical layer of Congestion Control networks.

3.3.3. Intentional Jamming Attack

This is one of the most basic types of attack that can be performed by secondary users.

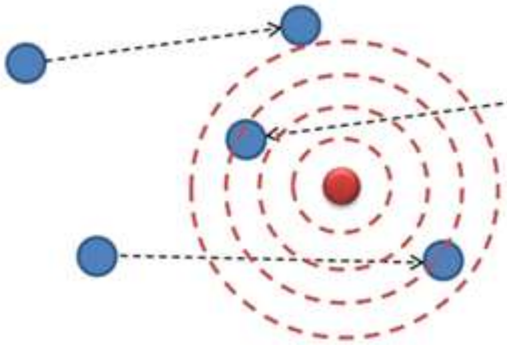

Fig. 6. International Jamming of connecting nodes

The attack can be further amplified by using high transmit power, transmitted in several bands. Although simple energy-based detection and triangulation techniques can be used to detect this attack, the time it takes to pinpoint and ban the malicious user impacts severely on the network performance.

3.3.4. Primary Receiver Jamming Attack

The attack is caused when a malicious entity closer to the victim primary receiver participates in a collaborative protocol and requests transmissions from other secondary users to be directed towards the malicious user.

3.3.5. *Sensitivity Amplifying Attack*

This leads to frequent false detections and missed opportunities for the secondary users. Operating in multiple bands to incur missed opportunities and render Band usage inefficient.

3.3.6. Overlapping Secondary User Attack

In both centralized and distributed Congestion Control networks, multiple secondary networks may coexist over the same geographical region.

In such cases, transmissions from malicious entities in one network can cause harm to the primary and secondary users of the other network. This type of attack is hard to prevent because the malicious entities may not be under the direct control of the secondary base station/users of the victim network.

3.3.7. Link Layer Attacks

The link layer provides Security Issues in Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Network the functional means to allow fragmentation of data, error correction and modulation. The medium access control (MAC) layer is one of the important sub layers of the link layer, which controls channel assignment.

3.3.8. Asynchronous Sensing Attack

Instead of synchronizing the sensing activity with other secondary users in the network, a malicious secondary user may transmit asynchronously when other secondary users are performing sensing operations. If the base station or other secondary users consider this as a transmission from a primary user, then this could result in missed opportunities. This attack can be made more efficient by transmitting only during sensing periods.

3.3.9. False Feedback Attack

False feedback from one or a group of malicious users could make other secondary users take inappropriate actions and violate the goals of the protocol. Primary base station's transmission range. A similar attack is possible in centralized Congestion Control radio network.

3.3.11. Network Layer Attacks

While the data link layer is responsible for node to node (one-hop) packet delivery, the network layer is responsible for end-to-end (source-to-destination) packet delivery. The network layer provides functional means for performing routing, flow control and ensuring quality of service (QoS). Some of the routing protocols used in wireless environment are for example dynamic source routing (DSR) and ad-hoc on demand distance vector (AODV) routing.

A malicious node in the path can disrupt routing by either broadcasting incorrect routing information to its neighbors or by redirecting the packets in the wrong direction. Several routing attacks have been discovered in wireless ad-hoc networks, most of the attacks can be classified into two categories: routing disruption attacks and resource consumption attacks. Some of the examples of routing attacks are the black hole attack where the malicious node attracts packets from every other node and drops all the packets, the gray hole attack where the malicious node selectively drops the packets, the worm hole attack where the malicious user uses two pairs of nodes with a private connection between the two pairs.

The worm hole attack is a dangerous attack since it can prevent route discovery where the source and the destination are more than two hops away. Most of these attacks are prevented by using secure on-demand routing protocols like secure AODV, which use cryptographic mechanisms to guarantee integrity of routing information and authenticity of nodes.

4.1.1. Future Directions

We provide some future directions that need to be taken to make secure Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks against both accidental and intentional attacks. Most of our Security Issues in Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks proposed solutions are easy to implement (for example, using existing security protocols).

4.1.2. Using Existing Security Protocols

Security services provided in cellular, WLAN and wireless ad-hoc networks can be applied to Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks as well. It is the last hop between the wireless base stations and the wireless terminals that needs to be protected over the air. Confidentiality is provided by using the confidentiality algorithm known as f8 and the secret cipher key (CK) that is exchanged as a part of the AKA process. Integrity is provided by using the integrity algorithm, f9 and the integrity key (IK). A block cipher known as KASUMI is the building block of both f8 and f9 algorithms. KASUMI operates on 64 bit blocks and uses a 128-bit secret key. Decentralized Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks could use security mechanisms employed in ad-hoc wireless networks.

4.1.3. Using Cryptographic Primitives

Primary user identification is very important for both centralized and decentralized Congestion Control networks. We recently proposed a digital signature based primary user identification mechanism that can be used by secondary users to distinguish malicious transmissions from primaries.

4.1.4. Reactive Security Mechanisms

Reactive security mechanisms that detect malicious activity in Cross Layer Design, For example, mechanisms that can detect unusually high Band handoffs is useful to prevent jamming and Band handoff attacks.

4.1.5. Band Aware Approach

There are two ways to handle Band mobility and associated delays. One is to make Band sensing, analyzing and handoff process fast and transparent to the higher layer protocols. However, Band sensing and handoff processes are in their infant stages and it will take a long time for such approaches to materialize. Another approach is a cross-layer methodology to incorporate Band mobility as state information in protocols operating in upper layers. Although this approach increases cross-layer dependencies on transport layer should consider the effect of Band handoff on the round trip time and correspondingly adjust the retransmission window.

4.1.6. Use Light-weight Security Protocols and Primitives

Light-weight security protocols need to be developed for power/resource constrained environments.

5. Conclusions

The main motivation behind Cross Layer design has been to increase Band utilization by allowing the unlicensed (secondary) users to opportunistically access the frequency band actually owned by the licensed (primary) user. In contrast to other network security architectures, the users are categorized into two distinct classes: primary users and secondary users. We also discussed various security aspects such as authentication and authorization of users, confidentiality and integrity of communication as well as identification and non repudiation of Congestion Control user devices. Some reliability issues that are inherent in cognitive networks were examined. Through these attacks we showed that the fundamental idea behind Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks (to have self-aware networks that offer resilient services and keep the intruders out of it simply by cognition) is yet fulfilled. Finally, we suggested some future directions that need to be taken to make the protocols that are employed in Cross Layer Design Approach for avoid Congestion Control in Wireless Mobile AD-HOC Networks.

6. References.

[1] T. S. Rappaport, A. Annamali, R. M. Buehrer, and W. H. Tranter, “Wireless Communications: Past events and a future perspective,” *IEEE Communications Magazine,* pp. 148-161, May 2002.

[2] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” In *the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking* (MobiCom'98), pages 85~97, October 1998.

[3] S.-J. Lee, M. Gerla, and C. -K. Toh, “A Simulation Study of Table-driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks,” *IEEE Network Magazine*, pp. 48-54, August 1999.

[4] E. M. Royer, S. J. Lee, and C. E. Perkins, “The effects of MAC protocols on ad hoc networks communication,” *Proc. of IEEE WCNC'00*, Vol. 2, pp. 543-548, September 2000.

[5] J.-H. Lee, S. Singh, and Y.-S. Roh, “Interlayer Interactions and Performance in Wireless Ad Hoc Network,” IRTF ANS Working Group, Internet-Draft, *draft-irtf-ans-interlayer performance-00.txt*, September 2003.

[6] W. H. Yuen, H.-no Lee and T. D. Andersen, “A Simple and Effective Cross Layer Networking System for Mobile Ad Hoc Networks,” *IEEE PIMRC,* Vol.4, pp.1952–1956, September 2002.

[7] Y.-C. Hu and D. B. Johnson, “Exploiting Congestion Information in Network and Higher Layer Protocols in Multihop Wireless Ad Hoc Networks,” In *the 24th International conference on Distributed computing Systems* (ICDCS 2004), pp.301-310, IEEE, Japan, March 2004.

[8] S. Shakkottai, T. S. Rappaport and P. C. Karlsson, “Cross-layer Design for Wireless Networks,” *IEEE Communications Magazine*, pp.74-80, October 2003.

Authors Profile

K.Priya did her M.Tech, M.Phil. In Computer Science and Engineering from JNTUK. A.P. INDIA. Her area of expertise includes Computer Networks, wireless LANs, IP address, routing algorithms, Information Technology. She is working as Lecturer in department of Computer Science at P.B. Siddhartha College of Arts and Science, Vijayawada, and Andhra Pradesh, India.

Dr. Ujwal A. Lanjewar, Ph.D., MCA, M.Sc. (Stats), MBA, Diploma in Industrial Engineering, Diploma in Export Management, is a Professor and Research Supervisor in the **Faculty** of Computer Science of R.T.M. Nagpur University, Nagpur. He was awarded as “Professor Raghvendra Rao Best Application Paper Award” in International Conference, 37th Annual Convention of ORSI held at IIM, Ahmadabad during Jan 8-11, 2005.

Ms K Prasuna Presently she is working as Assistant Professor in ECE department in Vijaya Institute of Technology for Women, Vijayawada. She has more than 5 years of teaching experience. Her areas of interest are Digital Signal Processing, Wireless Communications, Image Processing and Wireless Networks.

Chilakalapudi Meher Babu did his M.Tech Computer Science and Engineering from Nimra Institute of Science And Technology affiliated to Jawaharlal Nehru Technological University, Kakinada, and A.P. INDIA and pursuing Ph.D in R.T.M. Nagpur University, Nagpur.. His research areas Network Intursion Detection System on Wireless Mobile Ad-hoc Networks and Computer Networks, wireless LANs, IP address, routing algorithms.