International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 3, Issue 11 (June 2014) PP: 52-56

A Systematic Review of Congestion Control in Ad Hoc Network

M. Rajesh[1], Dr. J. M. Gnanasekar[2]
[1]*Research Scholar, Department of Computer Science & Engineering, St.Peter's University Chennai,*
[2]*Professor & Head Department of Computer Science & Engineering2, Karpaga Vinayaga College of Engineering & Technology*

Abstract: *Congestion is said to occur in the network when the resource demands exceed the capacity and packets are lost due to too much queuing in the network. During congestion, the network throughput may drop to zero and the path delay may become very high. A congestion control scheme helps the network to recover from the congestion state. In fact, security plays a vital role in Wireless Ad hoc network. This paper presents a systematic literature review to provide comprehensive and unbiased information about various current model Congestion Control conceptions, proposals, problems and solutions in Ad hoc for safety transportation. For this purpose, a total of 33 articles related to the security model in Congestion Control published between 2008 and 2013 were extracted from the most relevant scientific sources (IEEE Computer Society, ACM Digital Library, Springer Link and Science Direct). However, 18 articles were eventually analyzed due to several reasons such as relevancy and comprehensiveness of discussion presented in the articles. Using the systematic method of review, this paper succeeds to reveal the main security threats and Error control, challenges for security, security requirement in Congestion Control in Wireless Ad hoc network (CCWAN) and future research within this scope.*

Keyword: *Congestion control, Security, Error control, CCWAN, Systematic Literature Review.*

I. Introduction

The basic cause of congestion is that the input traffic demands exceed the capacity of the network in typical packet switching networks, this can occur quite easily when output links are slower than inputs and multiple traffic sources competing for same output link at the same time The Congestion control problem is more acute in ad hoc networks Congestion can happen faster in wireless networks.

Interconnecting high speed and lower speed networks creates congestion problems at the point of interconnect. There are two fundamental approaches to congestion control: reactive approaches and preventive approaches. Reactive: feedback- based - attempt to detect congestion, or the onset of congestion, and take action to resolve the problem before things get worse. Preventive: reservation-based - prevent congestion from ever happening in the first place, by reserving resources. Switches can detect the onset of congestion (e.g., buffers filling up) switches set a control bit in cell headers to indicate this congestion condition sources react by reducing the volume of traffic that they are sending through that switch.

A series of protocols have been introduced to supplement the insufficient TCP mechanism for controlling the congestion. As such the Core-Stateless Fair Queuing (CSFQ),Token based Congestion Control (TBCC) were designed as open or closed-loop controller respectively to provide the fair best effort service for supervising the per-flow bandwidth consumption. An adaptive location-based channel congestion control scheme for the V2I (Vehicle to Infrastructure) communication is proposed. The service channel (SCH) interval into exclusive access period (EAP) and contention access period. Innovative model and congestion control algorithm for wireless sensor networks based on feedback control, which will be referred to as Feedback Congestion Control (FBCC). The algorithm has been designed by exploiting linear discrete time control theory. The FBCC detects the onset of congestion using queue length.

Presently the Internet accommodates simultaneous audio, video, and data traffic. This requires the Internet to guarantee the packet loss thus to control network congestion. A series of protocols have been introduced to supplement the insufficient [1]. Scheduled approaches to channel access provide deterministic rather than probabilistic delay guarantees. This is important for applications sensitive to maximum delay. Furthermore, the control overhead and carrier sensing associated with contention MAC protocols can be considerable in terms of time and energy [2]. The challenge with scheduling is to achieve a reasonable throughput objective.

Two approaches have emerged to exploit spatial reuse in response to topology changes. Topology-dependent protocols alternate between a contention phase in which neighbor information is collected, and a scheduled phase in which nodes follow a schedule constructed using the neighbor information (see, as examples, [3], [4]). In contrast, the idea in Topology-transparent protocols is to design schedules that are independent of the detailed network topology. Specifically, the schedules do not depend on the identity of a node's neighbors, but rather on how many of them are transmitting. Even if a node's neighbors change its schedule does not; if the number of neighbors does not exceed the designed bound then the schedule still succeeds.

The existing topology-transparent protocols depend on two parameters. The number of nodes in the network, and, the maximum node degree. Chlamtac et al. [5] gave a construction based on Galois fields and finite geometries using the algebraic property that polynomials of bounded degree cannot have many roots in common; informally, their intersection is small. The schedules derived from the polynomials share the same intersection property and do not overlap in too many slots. In their scheme if a node has at most neighbors, there is at least one collision-free slot to each neighbor within a frame. Their focus was on parameters to minimize schedule length. Jute al. [6] argued that the parameters satisfying the condition on delay do not maximize the minimum throughput. They showed it is possible to achieve higher minimum throughput at the expense of longer frame length. Intuitively, while Chlamtac et al. strive to get one free slot to each neighbor per frame, Jute al. aim to get many slots to the same neighbor per frame. There are complex trade-offs between the design parameters and the delay and throughput characteristics of the resulting schedules [7].

The rest of this paper is organized as follows. Section II defines a cover-free family and examines orthogonal arrays as an important class of this family. We also derive the bound on expected throughput. Section III discusses acknowledgment schemes including RFEC for this purpose and overviews the LT process. Section IV describes an experiment that makes a direct comparison between the proposed RFEC scheme and the ideal scheme in which the transmitter is omniscient, in the sense that it receives acknowledgments instantaneously. Comparisons for achieved delay and throughput are presented. Section V addresses the greatest challenge for scheduling in dynamic environments, namely adaptation to changing network conditions. Finally in Section VI, we examine the potential use of topology transparent schemes in light of the practical acknowledgment scheme developed and discuss remaining limitations.

II. Model and Problem Formulation

An ad hoc network topology can be represented by an undirected graph whose vertices represent the network nodes, and where an edge between any pair of vertices represents radio proximity between two nodes. Due to such proximity, simultaneous transmissions often result in collisions. To model such interactions between links, from the topology graph, we can construct a link contention graph, where a vertex represents an active link, and an edge between two vertices denotes wireless proximity between the two links: that is, either the sender or the receiver of one link is within radio proximity of the sender or the receiver of the other.

Note that this contention graph only represents the contentions that occur within the carrier sensing range and neglects the additive nature of interference. A more accurate representation of contentions should take into account interference generated by all nodes in the network, however, since interference is additive, it can only be represented accurately by knowing the whole topology of the network, which is impractical in ad hoc networks. The cliques of the link contention graph represent accurately the time-domain bandwidth sharing constraints. That is, no two links in the same clique can be active simultaneously. Thus, each clique in the contention graph stands for a contention context, and is an accurate abstraction of a "channel resource" in the real network. Links in the same clique share the capacity of this channel resource according to the target fairness principle. So, from the bandwidth sharing viewpoint, a particular link succeeds transmission if and only if all other links in all the cliques containing this particular link do not transmit. Examining the problem from another viewpoint, links that form an independent set in the link contention graph can be scheduled to transmit simultaneously. While the search for cliques in a graph and the search for all independent sets of a graph are both NP hard, the latter is less appealing for ad hoc networks because independent sets are spatially distributed and thus require the knowledge of the global contention graph, and thus the whole network topology, whereas cliques are by nature local sub graphs of this global graph.

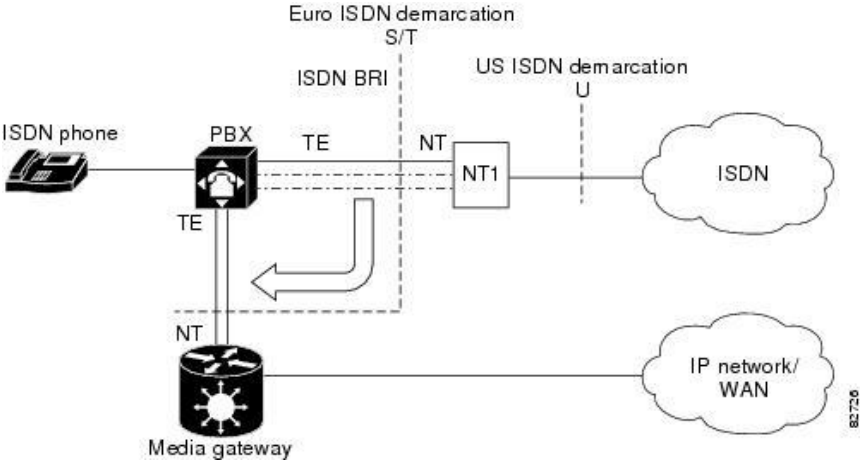

Figure 1 Typical ISDN BRI Network-Side Scenario

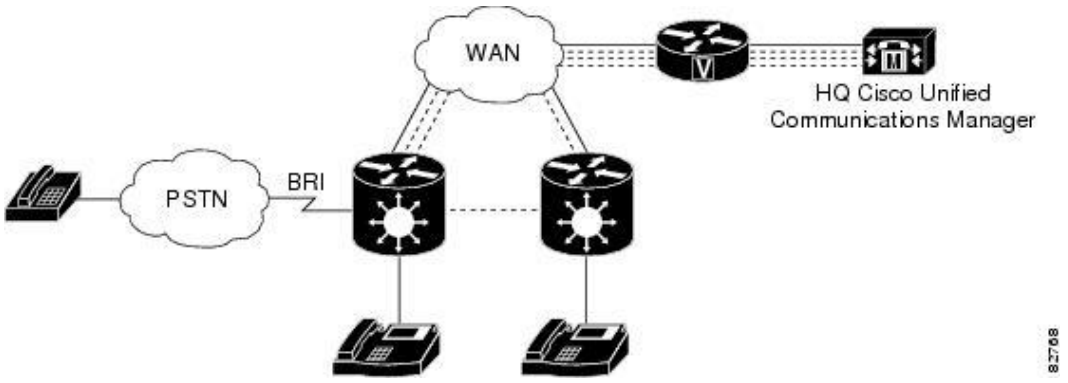

Figure 2 shows a typical user-side scenario.

III. Protocol and Network Management

In the network formation, nodes perform an initial exchange of configuration information and security using the mechanism of authentication. This mechanism avoids the need for a central server, making the tasks of building the network and adding new members very easy.

The network is created using the information provided by users, thus, each node is identified by an IP address. Services are shared using TCP connections. The network is built using IEEE 802.11b/g technology which has high data rates to share resources. We have reserved the short-range technology (Bluetooth) to allow authentication of nodes when they join the network.

After the authentication process, each node learns the identity card of other known nodes, a public key and a LID. This information will be updated and completed throughout the network nodes. This structure provides an authenticated service that verifies the integrity of the data from each node because there is a distributed CA.

Each node requests the services from all the nodes that it trusts, or from all known nodes in the network, depending on the type of service. A request to multiple nodes is made through diffusion processes. The protocol prioritizes access to information through trusted nodes. When the information cannot be obtained through these nodes, it can then ask other nodes.

Nodes can also send requests to update network information. The reply will contain the identity cards of all nodes in the network. The node replying to this request must sign this data ensuring the authenticity of the shipment. If it is a trusted node, its validity is also ensured, since trusted nodes have been responsible for validating their previous certificates. Under this network, any type of service or application can be implemented. The services offered by our protocol will be secure.

Network Creation

The first node in the network will be responsible for setting the global settings of the spontaneous network (SSID, session key, ...). However, each node must configure its own data (including the first node): IP, port, data security, and user data. This information will allow the node to become part of the network. After this data are set in the first node, it changes to standby mode.

The authenticated node can perform the following tasks:

- Display the nodes
- Modify the trust of the nodes.
- Update the information: It allows a node to learn about other nodes in the network and also to send its data to the network. This update could be for only one user or for all users in the network through a controlled diffusion process.
- Other nodes certificate request: A node could be requested from other node, from all trusted nodes or from all known nodes. In case of all known nodes, the node that replies to the request will always sign the data. The data will be considered validated if a trusted node has signed them.
- Process an authentication request: The node authenticates a requesting node by validating the received information, user authentication, and verifying the no duplication of the LID data and the proposed IP.
- Reply to an information request: the requested information will be sent directly to the requesting node or routed if the node is not on the communication range.
- Forward an information request: The request will be forwarded if it is a broadcast message
- Send data to one node: It can be sent symmetrically or asymmetrically encrypted, or unencrypted.
- Send data to all nodes: This process is doing by a flooding system. Each node retransmits the data only the first it receives the data. It can be sent symmetrically encrypted or unencrypted.

- Modify Data: User data can be modified and the password changed.
- Leave the network.

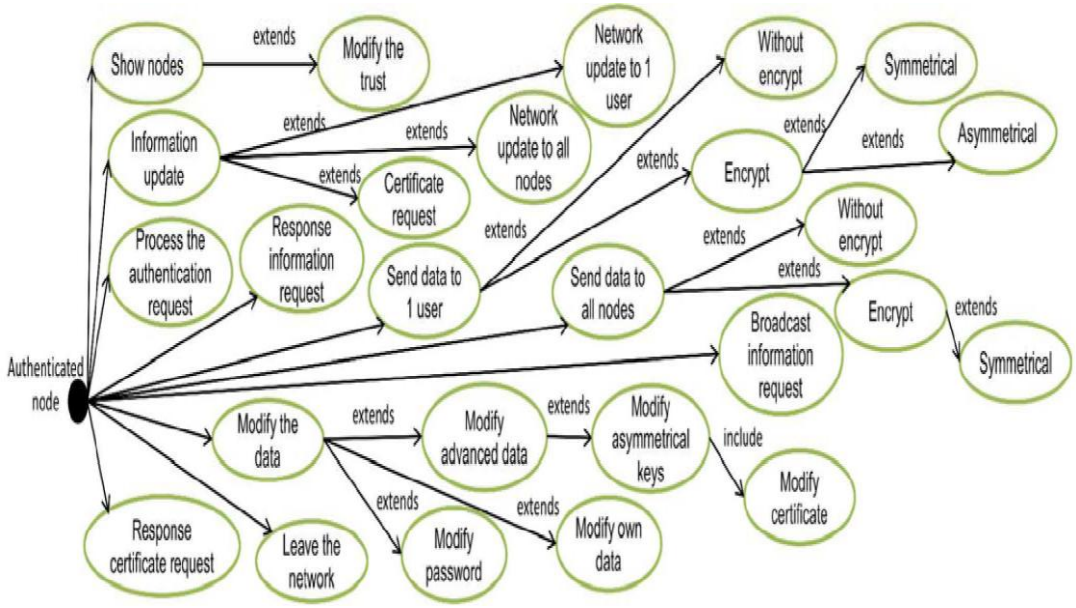

Figure 3. Node options after the authentication procedure

To request a certificate, the node sends a request certificate message to its trusted nodes. The application generates a packet to request the certificate to its trust nodes which are selected from the database.

IV. Conclusion

Due to the importance of Congestion Control for Wireless Ad hoc network, in this literature review, we analyze various studies focusing on Congestion Control in CCWAN. We found some of the treats and challenges related to CCWAN Congestion Control. Also, we obtain the requirements that are required for creating and designing a Congestion Control model. These security issues make a potential stumbling block to deploy CCWANs. From the analysis in survey, we came to know that there doesn't exist a comprehensive security protocol or framework that covers all security aspects of CCWAN. Therefore, it is necessary to develop a suitable framework which mitigates all these Congestion problems; more research is required in this area. Moreover, the impact of trust on Congestion Control in CCWAN is other objective in future works.

REFERENCES

[1] Zhiqiang Shi, Ionescu, D., Dongli Zhang, "A Token Based Method for Congestion and Packet Loss Control " Latin America Transactions, IEEE (Revista IEEE America Latina) (Volume:11 , Issue: 2) March 2013.

[2] A. Woo and D. E. Culler, "A transmission control scheme for media access in sensor networks," in Proc. MobiCom'01, Jul. 2001, pp. 221–235.

[3] Chlamtac and S. S. Pinter, "Distributed node organization algorithm for channel access in a multihop dynamic radio network," IEEE Trans. Comput., vol. 36, pp. 728–737, Jun. 1987.

[4] C. Zhu and S. Corson, "A five-phase reservation protocol FPRP for mobile ad hoc networks," in Proc. IEEE INFOCOM, 1998, pp. 322–331.

[5] I. Chlamtac and A. Faragó, "Making transmission schedules immune to topology changes in multi-hop packet radio networks," IEEE/ACM Trans. Networking, vol. 2, no. 1, pp. 23–29, Feb. 1994.

[6] J.-H. Ju and V. O. K. Li, "An optimal topology-transparent scheduling method in multihop packet radio networks," IEEE/ACM Trans. Networking, vol. 6, no. 3, pp. 298–306, Jun. 1998.

[7] C. J. Colbourn, A. C. H. Ling, and V. R. Syrotiuk, "Cover-free families and topology-transparent scheduling for MANETs," Designs, Codes,and Cryptography, vol. 32, no. 1–3, pp. 35–65, May 2004.

[8] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystem without Group Manager," Network Protocols and Algorithms,vol. 1, no. 1, Oct. 2009.

[9] J. Yan, J. Ma, F. Li, and S.J. Moon, "Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks," Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.

[10] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.

[11] K. Sahadevaiah and P.V.G.D. Prasad Reddy, "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140, 2011.

[12] L. Herrero and R. Lacuesta, "A Security Architecture Proposal for Spontaneous Networks," Proc. Int'l Conf. Advances in the Internet Processing System and Interdisciplinary Research, Oct. 2003.

[13] R. Lacuesta and L. Pen˜ aver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05), July 2005.

[14] R. Lacuesta and L. Pen˜ alver, "Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses," Proc. Int'l Conf. Emerging Security Information, Systems and Technologies (SECURWARE '07), 2007.
[15] J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.
[16] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[17] S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.
[18] J. Ba¨ckstro¨m and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.
[19] V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.
[20] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
[21] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC'05),Mar. 2005.
[22] J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.
[23] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-Aware People-Centric Sensing," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 17-20, June 2008.
[24] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "Two Secure and Energy-Saving Spontaneous Ad-Hoc Protocol for Wireless Mesh Client Networks," J. Network and Computer Applications, vol. 34, no. 2, pp. 492-505, Mar. 2011.
[25] J. Sun, C. Zhang, Y. Zhang, and Y. (Michael) Fang, "An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.