ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Efficient Estimation of Hybrid Wireless Networks using QoS-Oriented Distributed routing protocol

Priyananci.S [1], Suriya.M[2], Anandakumar.H[3], Anuradha.B[4]
Pg Scholar [1], Assistant Profosser[2], Assistant Professor[3], Associate Professor[4]
Department of Information Technology, SNS College of Engineering, Coimbatore.

Abstract

Hybrid networks are next generation of wireless networks which is a combination of Mobile ADHOC networks and Wireless Infrastructure networks. They are increasingly used in wireless communications that are highly supporting real time transmission with limited Quality of Service. When the transmission link breaks between source node and destination node invalid reservation problem occurs, and when same resource is allocated to two different QoS paths race condition problem occurs. In existing system QoS-Oriented Distributed routing protocol is used to enhance the QoS support capability of hybrid networks, it transforms the packet routing problem to resource scheduling problem which has five algorithms. They are, QoS guaranteed neighbour selection algorithm, Distributed packet scheduling algorithm, Mobility based segment resizing algorithm, Traffic redundant elimination algorithm and Data redundancy elimination based transmission algorithm. The main drawback of hybrid networks is so far examined in minimum transmission hops and has less beneficial feature with limited number of mobile access points, mobility speeds, and mobile workloads and with different network sizes. It can highly perform on random way point model and less in real mobility model. To increase the performance of hybrid networks in real mobility model a method can be proposed to authenticate data streams for transmission. Data Transparent Authentication without Communication overhead is an approach which reduces breakdown of original data or sends out of band authentication information. The future work can be done with increased transmission hops that can perform under various jitter patterns and find the packet loss on both UDP and TCP based data streams.

Keywords: Hybrid wireless networks, routing algorithm, quality of service, Data transparent authentication.

Introduction

Wireless networks have been developed with various wireless applications, which have been used in areas of commerce, emergency, services, military, education and entertainment. The rapid improvement of Wife capable mobile devices including laptops and handheld devices, for example the purpose of wireless internet users of smart phone in last three years. The usage of people watching video, playing games and making long distance video or audio conferencing through wireless mobile devices and video streaming applications on infrastructure wireless networks which connects directly to mobile users for video playing and interaction in real time are increased [1]. The evolution and the anticipate future of real time mobile multimedia streaming services are extensively expanded, so the networks are in need of high Quality of Service(QoS) to support wireless and mobile networking environment.

To improve the QoS support capability of hybrid network that are supported resource reservation based routing. Once the transmission link breaks between source node and destination node invalid reservation problem occurs, and once same resource is allotted to two totally different QoS methods race condition problem occurs [2]. However, very little effort has been dedicated to support QoS routing in hybrid networks. Most of the present works in hybrid networks concentrate on increasing network capability or routing dependability however cannot provide QoS-guaranteed services. Direct adoption of the reservation-based QoS routing protocols of

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

MANETs into hybrid networks inherits the invalid reservation and race condition issues.

QoS-Oriented Distributed routing protocol is used in hybrid network for data transmission , which has extensive base station with two main features. An Acess Point (AP) can be a source or destination and the number of transimission hops between mobile node and access poins is small. Acess point to any mobile nodes allow data streams to have any cast transmission alog with multiple transmission paths to its destination through base stations.

Its enables a source node to connect through an intermediate node in access point. Thus having two features QOD transforms the packet routing problem into a dynamic resource schedulling problem. If a source node is not within the transmission range of the AP, a source node selects nearby neighbours that can provide QoS services to forward its packets to base stations in a distributed manner. The source node schedules the packet streams to neighbours based on their queuing condition, channel condition, and mobility, the purpose is to reduce transmission time and increase network capacity. But still the guarantee of QOS remains an open problem.

At present QoS-Oriented Distributed routing protocol is used to enhance the QoS support capability of hybrid networks, it transforms the packet routing problem to resource scheduling problem which has five algorithms.

QoS guaranteed neighbour selection algorithm. The rule selects qualified neighbours and employs deadline-driven programming mechanism to ensure QoS routing.

Distributed packet scheduling algorithm. After qualified neighbours are known, this algorithmic program schedules packet routing. It assigns earlier generated packets to forwarders with higher queuing delays, while assigns a lot of recently generated packets to forwarders with lower queuing delays to decrease total transmission delay.

Mobility based segment resizing algorithm. The source node adaptively resizes every packet in its packet stream for every neighbour node in line with the neighbour's quality so as to extend the programming feasibility of the packets from the source node.

Traffic redundant elimination algorithm. An intermediate node forwards the packet with the first smallest amount time allowed to attend before being forwarded to resolute succeed fairness in packet forwarding.

Data redundancy elimination based transmission algorithm. Due to the broadcasting feature of the wireless networks, the access point and mobile nodes will cache packets. This algorithmic rule eliminates the redundant data to boost the QoS of the packet transmission.

Related work

MANETs

A majority of QoS routing protocols area unit supported resource reservation [9], within which a supply node sends probe messages to a destination to get and reserve ways satisfying a given QoS demand. Perkins et al. [10] extended the AODV routing protocol [11] by adding information of the most delay and minimum out there bandwidth of every neighbour during a node's routing table. Venataramanan et al. [12] projected a planning algorithm to make sure the tiniest buffer usage of the nodes in the forwarding path to BS. These works specialise in increasing network capability supported scheduling however fail to ensure QoS delay performance. Some works think about providing multipart routing to increase the strength of QoS routing.

Wireless sensor Networks

RAP [5] and SPEED [6] provides a high delivering priority to the packets with longer distance/delay to the destination. However, each strategy needs every device to grasp its own location, so they are not appropriate for extremely dynamic surroundings. Felemban et al. [7] and debutante et al. [8] projected to boost routing dependableness by multipath routing. However, the redundant transmission of the packets might result in high power consumption.

Hybrid wireless Networks

Very few ways are planned to produce QoS secured routing for hybrid networks. Most of the routing protocols solely attempt to improve the network capability and dependableness to indirectly give QoS service however bypass the constraints in QoS routing that need the protocols to produce secured service. Yufei et al [3] introduced relay selection scheme for improving the performance of hybrid

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

wireless network to improve network life time, error propagation and spectral efficiency.
Unlike the on top of works, QOD aims to supply QoS secure routing. QOD totally takes advantage of the widely deployed APs, and novelty treats the packet routing problem as a resource programming drawback between nodes and APs. To limit the throughput in wireless networks the two major factors are co-channel inference and unreliability. Kai Zeng et al [4] proposed Multi radio Multi Channel Opportunistic Routing scheme to improve the network throughput capacity to eliminating the limitation of the above factors.

This process can be done by optimizing the end-to-end throughput in linear programming using feasible scheduling of resources for achieving network capacity. The various comparisons of issues in Hybrid Networks, The architecture are Hybrid Wireless Network (HWN), Multi-Power Architecture for Cellular networks (MuPAC), Throughput enhanced Wireless in Local Loop (TWiLL), and Mobile Assisted Data Forwarding (MADF) see the table.1 below.

Issue	HWN	MuPAC	TWiLL	MADF
Routing Efficiency	Low	High	High	High
Routing Complexity	High	Low	Low	High
Connection or Packet based	Packet	Both	Connection	Both
Real-Time Traffic Support	Cellular Mode	Yes	Yes	Yes
Multiple Interfaces	Yes	Yes	Yes	No
Control Overhead	High	High	Low	High
Technology Dependent	No	No	No	No

Table 1. Comparison of hybrid wireless architectures

Infrastructure Networks

Existing approaches for providing warranted services in the infrastructure networks are supported 2 models: integrated services (IntServ) [13] and differentiated service (DiffServ) [14]. IntServ could be a state full model that uses resource reservation for individual flow, and uses admission management [13] and computer hardware to take care of the QoS of traffic flows. In contrast, DiffServ could be a unsettled model that uses coarse-grained class-based mechanism for traffic management. A number of queuing programming algorithms are proposed for DiffServ to additional minimize packet dejection and information measure consumption [13], [14], [15] Stoica et al. [16] projected a dynamic packet service (DPS) model to provide unicast IntServ-guaranteed service and DiffServ like scalability.

System model

In Data Transparent Authentication, the authentication unit could be an information block and also the authentication code is generated to support the content of the data block, referred to as Block Authentication Code (BAC). At the sender aspect, the authentication information BAC is to generate with supported a particular hash function with the packet content and a usually agreed key as the input, supported the worth of every bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays. At the receiver aspect, the receiver extracts the embedded BAC pack bit supported the relative packet delay and compares the extracted BAC with the BAC generated based mostly on the received content for authentication.

Thus, the proposed scheme consists of the Packet Selection using BAC generation, Mobility Based packet Resizing, Redundant Packet Elimination, Packet Authentication and Transmission. To describe the small print of those elements Efficient Estimation and Retransmission is mentioned with regard to packet loss, packet fragmentation, and out-of-order delivery. The proposed scheme uses the following notations:

1. The stream packets are clustered to blocks, denoted as block[p], with c packets in each block, where $0 < p <$ [tot_packet_no/c]. Padding is used when necessary to generate the last block.
2. The length (in terms of bits) of the BAC for each data block is m.
3. A hash function, denoted as H(Y), is a one-way hash, using an algorithm such as MD5 or SHA.
4. Q, R represents the concatenation of Q with R.
5. A secret key S is only known to the communicating parties.
6. The origin of the data stream can be identified by a flag, which is g bits, where $0 \leq g \leq m$.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

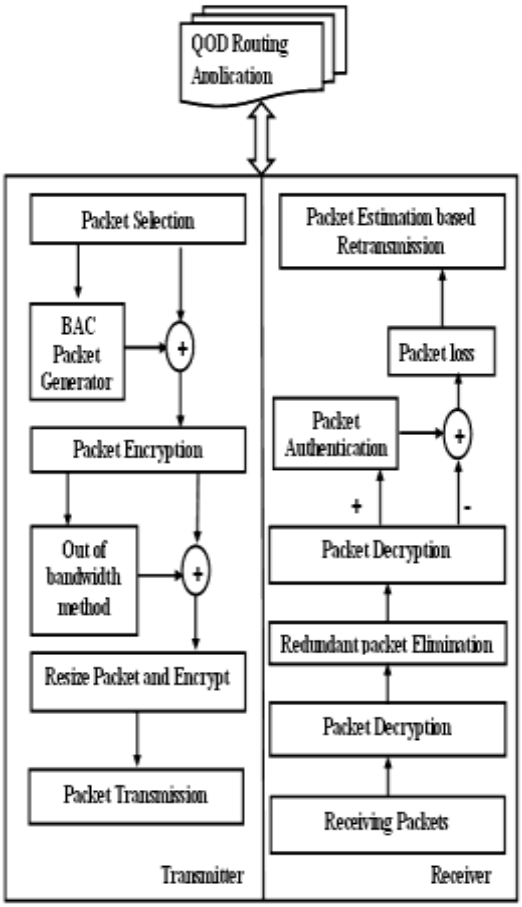

Figure 1. System Architecture

Module implementation

Packet Selection using BAC generation

In sender, the authentication information Block Authentication Code (BAC) is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays. Fig. 2 sketches the BAC generation procedure. The BAC generation for data block p involve three steps:

1. The concatenation of data block p and the secret key s is used as input to hash function H to generate a binary string of m + & bits, where & = m – g, string is said to be the first-breakdown.

2. The source flag, denoted as g, is concatenated to the generated bit in the previous step to get a binary string of 2m bits, said to be the second-breakdown.

3. The first m bits of the binary string are XOR_{ed} with the last m bits of the block p- first binary string, the result, BAC[p], is the final BAC for data blocks p.

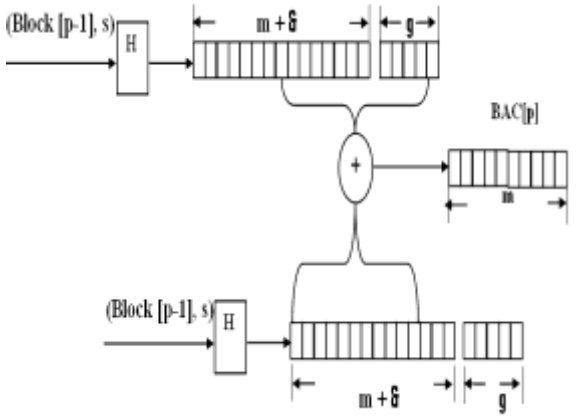

Figure 2. BAC Generation

In this BAC generation algorithm, if the values vary of & while keeping the & +g=m, they have different strategies.

1. &=0, When & is 0, the strategy becomes easy and straight forward. There is no chain at all. It only demands a fixed sized buffer of c packets at the sender side and the receiver side.

The strategy can detect packet alteration or addition and can locate changes in the granularity of a block. However, it cannot detect block deletion and block (burst packet) loss, which are very important in some stream-based applications, such as streaming media delivery, since streaming media data delivery normally runs on UDP.

2. &=m, When & is m, the strategy cannot authenticate the source. With more bits (2m) in the authentication code, the strategy reduces the collision rate since the number of bits in the hash result is larger. However, it has a problem due to chaining.

For example, if the verification of the current data block indicates that the current block is changed, it means that the hash value of the current block cannot be used to authenticate the next block. Thus, the authentication of the next block and all its subsequent blocks will be uncertain. In addition, the protocol cannot distinguish the change of a data block and the deletion (or loss) of a data block. The choices of & and g have the trade-off between authenticating the source and chaining to determine if the preceding block is lost. In most of existing hash-chain-based strategies, & is m, or the hash function takes the two consecutive blocks as the input. This causes their authentication deficiency. Thus, an appropriate & should satisfy $0 < \& < m$.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Conclusion

Data streams have been used in many Internet applications, such as grid computing and streaming media. More and more applications like these demand a reliable and effective authentication mechanism to ensure the genuineness of data streams transferred over the Internet. Although plenty of research work has been conducted, existing work shares the characteristics of either slightly changing the original data, or sending the authentication information out-of-band, neither of which is desirable when the data carry sensitive information or when the data are transmitted to mobile devices. To increase the performance of hybrid networks in real mobility model a method can be proposed to authenticate data streams for transmission. Data Transparent Authentication without Communication overhead is an approach which reduces breakdown of original data or sends out of band authentication information. The future work can be done with increased transmission hops that can perform under various jitter patterns and find the packet loss on both UDP and TCP based data streams.

References

[1] H. Wu and X. Jia, "QoS Multicast Routing by Using Multiple Paths/Trees in Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 5, pp. 600-612, 2009. (2002).

[2] Jawhar and J. Wu, "Quality of Service Routing in Mobile Ad Hoc Networks," Network Theory and Applications, Springer, 2004.

[3] Yifei Wei, F. Richard Yu, Senior Member, IEEE, and Mei Song "Distributed Optimal Relay Selection in Wireless Cooperative Networks with Finite-State Markov Channels" IEEE Trans. Veh. Technol., vol.59, no.5, June 2010.

[4] Kai Zeng, Member, IEEE, Zhenyu Yang, Student Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Opportunistic Routing in Multi-Radio Multi-Channel Multi-Hop Wireless Networks" IEEE Trans. Wireless Comm. Vol. 9. No. 11.Novmber 2010.

[5] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, "RAP: AReal-Time Communication Architecture for Large-Scale Wireless Sensor Networks," Proc. IEEE Real-Time and Embedded Technology Applications Systems, 2002.

[6] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks," Proc. 23rd Int'l Conf. Distributed Computing Systems, 2003.

[7] E. Felemban, C. Lee, and E. Ekici, "MMSPEED: Multipath Multi-Speed Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 738-754, June 2006.

[8] B. Deb, S. Bhatnagar, and B. Nath, "ReInForm: Reliable Information Forwarding Using Multiple Paths in Sensor Networks," Proc. IEEE 28th Ann. Int'l Conf. Local Computer Networks, 2003.

[9] I. Jawhar and J. Wu, "Quality of Service Routing in Mobile Ad Hoc Networks," Network Theory and Applications, Springer, 2004.

[10] C.E. Perkins, E.M. Royer, and S.R. Das, Quality of Service in Ad Hoc On-Demand Distance Vector Routing, IETF Internet draft, 2001.

[11] C. Perkins, E. Belding-Royer, and S. Das, Ad Hoc on Demand Distance Vector (AODV) Routing, IETF RFC 3561, 2003.

[12] Venataramanan, X. Lin, L. Ying, and S. hakkottai, "On Scheduling for Minimizing End-to-End Buffer Usage over Multi- Hop Wireless Networks," Proc. IEEE INFOCOM, 2010.

[13] R. Braden, D. Clark, and S. Shenker, Integrated Services in the Internet Architecture: An Overview, IETF RFC 1633, 1994.

[14] Y.E. Sung, C. Lund, M. Lyn, S. Rao, and S. Sen, "Modeling and Understanding End-to-End Class of Service Policies in Operational Networks," Proc. ACM Special Interest Group Data Comm. (SIGCOMM), 2009.

[15] J. Kurose and K. Ross, Computer Networking: A Top-Down Approach Featuring the Internet. Addison Wesley, 2004.

[16] I. Stoica and H. Zhang, "Providing Guaranteed Services without Per Flow Management," Proc. ACM Special Interest Group Data Comm. (SIGCOMM), 1999.