Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

# DATA TRANSPARENT AUTHENTICATION USING QOD IN HYBRID NETWORKS

D.J.Muthamizh[1], P.E.Prem[2], Dr.M.Akila[3]
[1] PG Scholar, Department of Information Technology
[2]Assistant Professor, Department of Information Technology
[3]Assistant Professor, Department of Information Technology
Vivekanandha College of Engineering for Women

**Abstract**— Hybrid networks are next generation of wireless networks that could be a combination of Mobile wireless adhoc (MANET) networks and Wireless Infrastructure networks. They are increasingly utilized in wireless communications that are extremely supporting real time transmission with restricted Quality of Service. Invalid reservation and race condition issues happens in MANET. In existing system, QoS-Oriented Distributed routing protocol (QOD) is employed to boost the QoS support capability of hybrid networks, it transforms the packet routing problem to resource scheduling problem that has 5 algorithms. They are, QoS guaranteed neighbor 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 restricted number of mobile access points, mobility speeds, and mobile workloads and with different network sizes. It will extremely perform on random way point model and less in real mobility model. This paper present Data Transparent Authentication to authenticates data streams by adjusting interpacket delay. Data Transparent Authentication while not Communication overhead is an approach which reduces breakdown of original information or sends out of band authentication data.

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

## I. INTRODUCTION

Wireless networks have been developed with numerous wireless applications, that are employed in in areas of commerce, emergency, services, military, education and entertainment. The fast development of Wi-Fi capable mobile devices together with laptops and hand-held devices, an example the aim of wireless net users of sensible phone in last 3 years. The usage of individuals looking video, taking part in games and creating long distance video or audio conferencing through wireless mobile devices and video streaming applications on infrastructure wireless networks that connects on to mobile users for video playing and interaction in real time area unit exaggerated [1].Hybrid networks mix wireless infrastructure networks and MANET. Infrastructure networks improve the scalability of MANET. MANET automatically establish self- organizing networks, extends the coverage the infrastructure networks[1].

 

The evolution and therefore the anticipate way forward for real time mobile multimedia system streaming services area unit extensively enlarged, that the networks area unit in would like of high Quality of Service(QoS) to support wireless and mobile networking environment.

To improve the QoS support capability of hybrid network that supported resource reservation based routing. Though these protocols will increase the QoS of the MANETs to an explicit extent, they suffer from invalid reservation and race condition issues. Invalid reservation issue happens once the transmission path breaks between source node and destination node. Race condition issue happens once double allocation of the same resource to 2 different QoS paths[2]. However, very little effort has been dedicated to support QoS routing in hybrid networks. Most of this works in hybrid networks focus on increasing network capability or routing reliability but cannot offer QoS-guaranteed services.

QoS-Oriented Distributed routing protocol is employed in hybrid network for data transmission , taht 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 attach 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 among the transmission range of the AP, a source node selects close neighbours that may offer 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 aim is to cut back transmission time and increase network capability. But still the guarantee of QOS remains an open problem.

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

- QoS secure neighbour selection algorithm: The rule selects qualified neighbours and employs deadline-driven programming mechanism to confirm QoS routing.
- Distributed packet scheduling algorithm: After qualified neighbours are known, this rule schedules packet routing. It assigns earlier generated packets to forwarders with higher queuing delays, whereas 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 each packet in its packet stream for each neighbour node in line with the neighbour's quality therefore on extend the programming feasibility of the packets from the source node.
- Traffic redundant elimination algorithm: An intermediate node forwards the packet with the primary least 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.

## II. RELATED WORKS

### 2.1 Hybrid wireless Networks

Very few ways are planned to produce QoS secured routing for hybrid networks. Most of the routing protocols entirely decide to improve the network capability and reliability to indirectly provide QoS service but bypass the constraints in QoS routing that require the protocols to produce secured service. Yufei et al [3] introduced relay selection scheme for rising the performance of hybrid wireless network to boost network life time, error propagation and spectral potency.

Unlike the on top of works, QOD aims to provide QoS secure routing. QOD entirely 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 2 major factors are co-channel inference and unreliability. Kai Zeng et al [4] projected Multi radio Multi Channel expedient Routing scheme to boost the network throughput capacity to eliminating the limitation of the higer than factors.

This method will be done by optimizing the end-to-end throughput in applied math victimisation possible scheduling of resources for achieving network capacity. The varied 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 Complexiy | High | Low | Low | High |
| Connection or Packet based | Packet | Both | Connection | Both |
| Real-Time Traffic Support | CellularMode | 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

 

### 2.2 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 may lead to high power consumption.

### 2.3 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 desiging rule to create certain the tiniest buffer usage of the nodes within the forwarding path to Base Station. These works specialize in increasing network capability supported scheduling, but fail to confirme QoS delay performance. Some works admit providing multipart routing toextend the strength of QoS routing.

### 2.4 Infrastructure Networks

Existing approaches for providing guaranteed services within the infrastructure networks area unit supported 2 models: integrated services (IntServ) [13] and differentiated service (DiffServ) [14]. IntServ can 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 can 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 supply unicast IntServ-guaranteed service and DiffServ like scalability.

## III. EXISTING SYSTEM

A QoS-oriented Distributed routing protocol (QOD).Usually, a hybrid network has widespread base stations. The data transmission in hybrid networks has 2 options, First, an AP will be a source destination to any mobile node, Second, the quantity of transmission hops between a mobile node and an AP is small. The first feature allows a stream to have any cast transmission along multiple transmission paths to its destination through base stations and the second feature enables a source node to connect to an AP through an intermediate node. Taking full advantage of the two features, QOD transforms the packet routing problem into a dynamic resource scheduling problem. Specifically, in QOD, if a source node is not within the transmission range of the AP, a source node selects a nearby neighbors that can provide QoS services to forward its packets to base stations in a distributed manner. The source node schedules the packet streams to neighbors based on their queuing condition, channel condition, and mobility, aiming to reduce transmission time and increase network capacity. The neighbors then forward packets to base stations, which further forward packets to the destination. We focus on the neighbor node selection for QoS-guaranteed transmission. QOD is the first work for QoS routing in hybrid networks.

 

## IV. PROPOSED WORK

We propose a completely unique methodology ,data-transperant Authentication(DaTA) while not communication overhead, to evidence the data streams. Our strategy neither embeds a digest to the original data, nor sends any out- of band authentication information. Instead, our scheme relies on the temporal order correlation of data packets between the sender and therefore the receiver. Notably, the inter packets delays area unit utilized and few chosen packets delays are slightly adjusted (in a range). The inter packet delay increase and reduce represent totally different bits (0 or1), and thus, transparently embed the digest. Since we limit the delay adjustment in a small range and the delay adjustment is not cumulative, the application's performance is hardly affected. Furthermore, our authentication strategy is no fragile , which can continuously authenticate the data stream even if a preceding data block is tampered with, and thus, provides stronger tamper detection capability at the block level. Modeling- based analysis revels how the false positives and false negatives of our proposed scheme can be trusted. To evaluate our proposed scheme ,we have implemented a prototype system and evaluated the system in an LAN and over the internet. In the LAN, the experiments are preformed under the various network jitter patterns including normal and burst, packet loss on both UDP and TCP based streams.

## V. SYSTEM MODEL

In Data Transparent Authentication, the authentication unit can be an information block and conjointly the authentication code is generated to support the content of the info block, referred to as Block Authentication Code (BAC). At the sender aspect, the authentication information BAC is to come up with supported a specific hash function with the packet content and a usually agreed key as the input, supported the value oh each bit (0/1) of BAC, some packets area unit 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 tiny print of these elements Efficient Estimation and Retransmission is mentioned with relevancy packet loss, packet fragmentation, and out-of-order delivery. The proposed scheme uses the subsequent 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 $0 \leq g \leq m$.

 

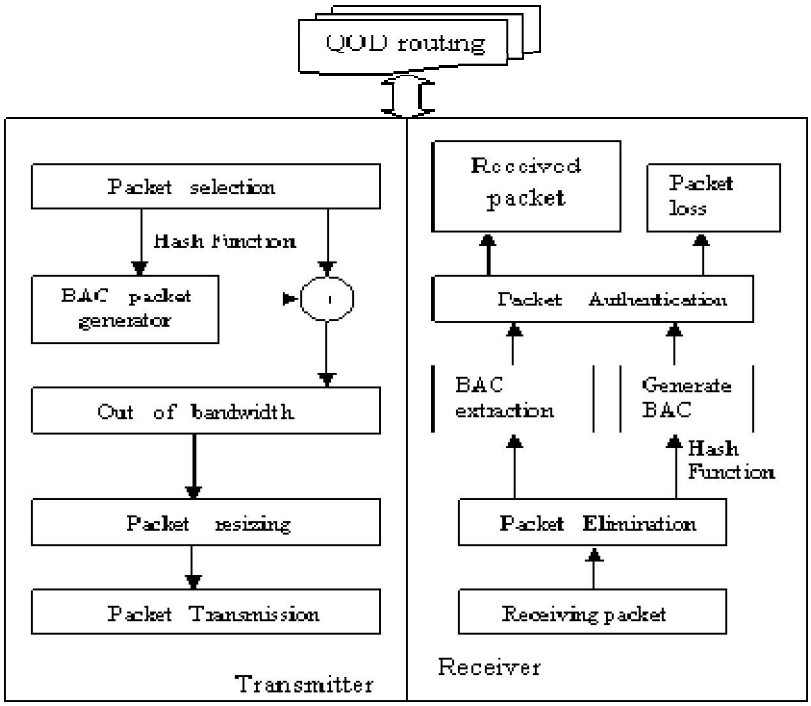


Figure 1. QOD Communication architecture

## V.CONCLUSION

Data streams are utilized in several web applications, like grid computing and streaming media. More and more applications like these demand a reliable and effective authentication mechanism to make sure the genuineness of data streams transferred over the web. Though many analysis work has been conducted, existing work shares the characteristics of either slightly ever-changing the original data, or sending the authentication info out-of-band, neither of that is fascinating once the data carry sensitive information or once the info transmitted to mobile devices. To extend the performance of hybrid networks in real quality model a technique is proposed to evidence information streams for transmission. Data Transparent Authentication while not Communication overhead is an approach that reduces breakdown of original information or sends out of band authentication data.

## 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] I. 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.

 