A QOS ORIENTED BAC TECHNIQUE FOR HYBRID NETWORKS

[1]Tamizharasi.V, [2]K.Kavitha
[1]Research Scholar, Department of Computer Science, Hindusthan College Of Engineering and Technology, Coimbatore.
[2]Assistant Professor,Department of Computer Science, Hindusthan College Of Engineering and Technology, Coimbatore.

Abstract: As wireless communication gains popularity, significant research has been devoted to supporting real-time transmission with stringent Quality of Service (QoS) requirements for wireless applications. At the same time a wireless hybrid network that integrates a mobile wireless ad hoc network (MANET) and a wireless infrastructure network has been proven to be a better alternative for the next generation wireless networks. By directly adopting resource reservation-based QoS routing for MANETs, hybrids networks inherit invalid reservation and race condition problems in MANETs. How to guarantee the QoS in hybrid networks remains an open problem. In the existing system propose a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks. Taking advantage of fewer transmission hops and any cast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. We propose a novel method, Data-Transparent Authentication (DaTA) without Communication Overhead, to authenticate data streams. Our strategy neither embeds a digest to the original data, nor sends any out-of band authentication information. Instead, our scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). The inter packet delay increase and decrease represent different bits (0 or 1) and thus transparently embed the digest. Since limit the delay adjustment in a small range and the delay adjustment is not cumulative, the application's performance is hardly affected.

1. INTRODUCTION

A QoS-Oriented Distributed routing protocol (QOD). Usually, a hybrid network has widespread base stations. The data transmission in hybrid networks has two features. First, an AP can be a source or a destination to any mobile node. Second, the number 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 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.

Propose a novel method, Data-Transparent Authentication (DaTA) without Communication Overhead, to authenticate data streams. Our strategy neither embeds a digest to the original data, nor sends any out-of band authentication information. Instead, our scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). The inter packet delay increase and decrease represent different bits (0 or 1), 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. 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 reveals how the false positives and false negatives of our proposed scheme can be tuned. 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 performed under various network jitter patterns including normal and burst, and packet loss on both UDP- and TCP-based streams.

The results show that the proposed scheme is robust to packet loss and can succeed when various network jitter patterns exist.

Little impact is found on the performance of the application. Over the Internet, the experiments are performed on nodes with 16-hop distance.

2. **RELATED WORK**

Provisioning of Adaptability to Variable Topologies for Routing Schemes in MANETs The routing *algorithm* used .But includes the multimedia, multi data rate, multi error rate case. The disadvantages of MANET are as following: It has limited resources. It has lack of authorization services. Topology changes frequently. These hybrid networks offer several advantages for users as well as operators.

Load Balancing and Resource Reservation in Mobile Ad-Hoc Networks Hence while simulating the QoS version of our algorithm, we let k=2.Thus 1/3 rd bandwidth is implicitly reserved for rerouted flows. The VMAC algorithm is a Virtual MAC algorithm that runs in parallel to the MAC algorithm on a mobile host, and estimates MAC-level statistics related to service quality. Increasing the number of links increase the contention at the MAC layer. It takes a long time to find all the paths and shares the time slots between the neighboring nodes. Using multiple paths provide high aggregate of the network bandwidth. High access rates and high stability due to using multiple path lantern trees.

Security and Quos Self-Optimization in Mobile Ad Hoc Networks using Optimization algorithm and QoS algorithm. Appropriate for a particular application environment. The security in routing protocols addressed in the recent past decade. Have compared these protocols by highlighting their features, differences and characteristics. It can be summed up that each protocol

Cooperative Communications with Relay-Selection When to Cooperate and Whom to Cooperate With Only partial CSI is needed for this proposed algorithm. By substituting the diversity order of the proposed algorithm is N + 1. The space diversity has widely been acknowledged, and as one kind of space diversity techniques, multiple input–multiple output (MIMO) has been incorporated into recent wireless standards. Digital processing and avoids noise amplification. The authors proposed in a distributed relay selection scheme that requires limited network knowledge with instantaneous SNRs.

A Simple Cooperative Diversity Method Based on Network Path Selection using the Distributed space–time coding algorithms. Here authors say that the variation in delivery times is 1/4 of other ad hoc networks, and ascribe this to the algorithm's use of best available delivery times. The authors arranged the test so that the protocol accumulates large blocks of data for transmission. Each packet is retransmitted a minimal number of times, and covers the longest possible distance on each transmission. Some time is wasted by having the receiver broadcast packet information, but this is far less than the normal routing schemes, which can retransmit when an acknowledge message is lost.

Semi-Distributed Relay Selection Algorithm for Multi-User Cooperative Wireless Networks using Relay selection algorithm is used. Cooperative communications for wireless networks have gained extensive interests due to their better capacity, coverage and reliability without requiring significant infrastructure deployment costs. The disadvantages of the clustering results correlate with the parameters of algorithm, the initial cluster centers, the input sequence of data patterns, and more required prior parameters.

Multi-rate relaying for performance improvement in IEEE 802.11 WLANs using the Adaptation *algorithm.*

First, ORP does not rely on RSSI data to discover relay nodes, avoiding the overhead of maintaining RSSI observations for each potential relay. We believe that transmit rate estimation based on RSSI is less straightforward than suggested in previous work. A signal of intent must be sent every time a computer wants to transmit causing signal traffic. Inappropriate for large/active networks, the slowdown increases, as the network grows larger. Limited; suffers from same distance limitations as CSMA/CD since it must listen for the signals of intent.

Dynamics of Random Early Detection used Early Random Drop algorithm. Association for Computing Machinery. Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial and those copies bear this notice and the full citation on the first page. A TCP connection that uses less than the fair share will reduce its congestion window on a single packet loss. In general, TCP connections with fewer buffers are at a disadvantage competing with other connections.

The Power of Prediction: Cloud Bandwidth and Cost Reduction They are three types algorithms. The pack algorithm, the Recursive algorithm and the sender algorithm. Over sender-based TRE, especially when the cloud computation cost and buffering requirements are important. Moreover, PACK imposes additional effort on the sender only when redundancy is exploited, thus reducing the cloud overall cost. Cloud providers cannot benefit from a technology whose goal is to reduce customer bandwidth bills, and thus are not likely to invest in one. The rise of on-demand work spaces, meeting rooms, and work-from-home solutions detaches the workers from their offices.

On Scheduling for Minimizing End-to-End Buffer Usage over Multichip Wireless Networks using Aβ-scheduling algorithm and scheduling algorithm. The hybrid algorithms perform much better than either the = 1, β 1 or the $\alpha = 1$, $\beta = 10$ algorithm. Also, both hybrid algorithms have similar performance which suggests that there is no advantage to decrease α further. Scheduling for WiMax mesh network Scheduling for broadband wireless access system. Guaranteed Rate Internet Traffic Delivery

A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: The Single-Node Case An RSVP-like *algorithm* can be *used* to reserve bandwidth and buffer space in an IP-router. The Leaky Bucket is described and proposed asa desirable strategy for admission control. Over our approach: it provides better jitter control and is probably easier to implement. A finite number of connection types are defined, where a type g connection is characterized by a fixed frame size of Tg. Color information is not propagated across backbone and must be configured manually. If subnets are split, a bridged path has to be set up between switches.

3. PROPOSED SYSTEM

In this propose method a novel method, Data-Transparent Authentication (DaTA) without Communication Overhead, to authenticate data streams. Our strategy neither embeds a digest to the original data, nor sends any out-of band authentication information. Instead, our scheme is based on the timing correlation of data packets between the sender and the receiver. Particularly, the inter packet delays are utilized and some selected packet delays are slightly adjusted (in a range). The inter packet delay increase and decrease represent different bits (0 or 1), and thus, transparently embed the digest.

Since limit the delay adjustment in a small range and the delay adjustment are 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 reveals how the false positives and false negatives of our proposed scheme can be tuned. To evaluate our proposed scheme have implemented a prototype system and evaluated the system in an LAN and over the Internet. In the LAN, the experiments are performed under various network jitter patterns including normal and burst, and packet loss on both UDP- and TCP-based streams.

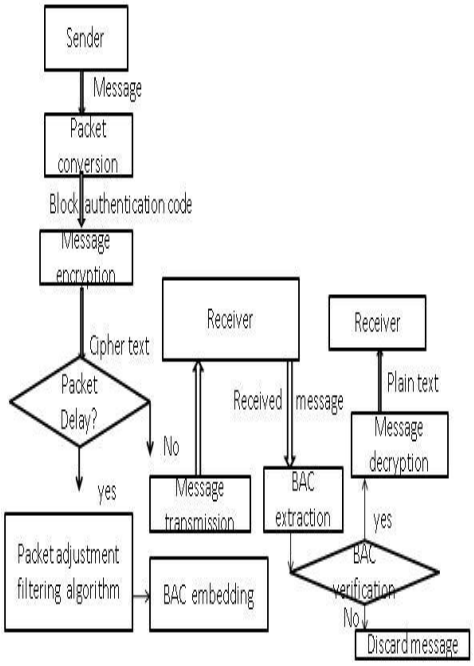


Figure: Architecture Diagram

- **Advantages**

The results show that the proposed scheme is robust to packet loss and can succeed when various network jitter patterns exist.

Little impact is found on the performance of the application. Over the Internet, the experiments are performed on nodes with 16-hop distance.

3.1 BAC ALGORITHM

- **Authentication:**

In Data, the authentication unit is a data block and the authentication code is generated based on the content of the data block, thus called Block Authentication Code (BAC). Data works as follows: At the sender side, the authentication information—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.

At the receiver side, the receiver extracts the embedded BAC based on the relative packet delay and compares the extracted BAC with the BAC generated based on the received content for authentication. Thus, our proposed scheme consists of the BAC generation, BAC embedding/BAC extraction and BAC authentication. In this section describe the details of these components. Packet boundary recognition issue is discussed with regard to packet loss, packet fragmentation, and out-of-order delivery then. An algorithm for the computation of a free resolutions is called sequential if it uses the sequence of generators as first criterion for ordering the pair sets. This means, it extends recursively a resolution.

$n - 1$ first generators to a resolution of n generators of a given ideal.

Algorithm : Sequential Search (A[1 .. n], key)
Input : An array A of n integers and an integer key
Output : A position of the key in the array (-1 if not found)

- **Project Description**

Node Configuration Setting

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes

- **Nodes Unique Identity**

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

- **Message Exchange Process for Route Discovery**

This module states a 4 step message exchange process i,e POLL, REPLY, REVEAL, REPORT. As soon the protocol executed the, POLL and REPLY messages are first broadcasted by Source and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless

medium, allowing nodes to record reciprocal timing information without disclosing their identities

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

- **BAC Generation**

The sender side, the authentication information 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.

- **BAC Embedding/Extraction**

After the BAC is generated, the next step is to embed the BAC. Different from existing strategies where the authentication information is sent out-of-band or embedded into the original data before data transmission, in DaTA, the

BAC is embedded by adjusting the inter-packet delay. In the following context present how the BAC bits can be embedded and extracted without touching the content of the packet.

To extract the BAC, the receiver calculates Yr; d as it receives the data packets. To extract an embedded bit, the receiver checks whether Yr; d is less than or greater than 0. The extraction of embedded binary bit is 1 if the value of Yr;d is greater than 0, or 0 if the value of Yr;d is less than or equal to 0. It is easy to see that probability of correct extraction is always greater than that of wrong extraction.

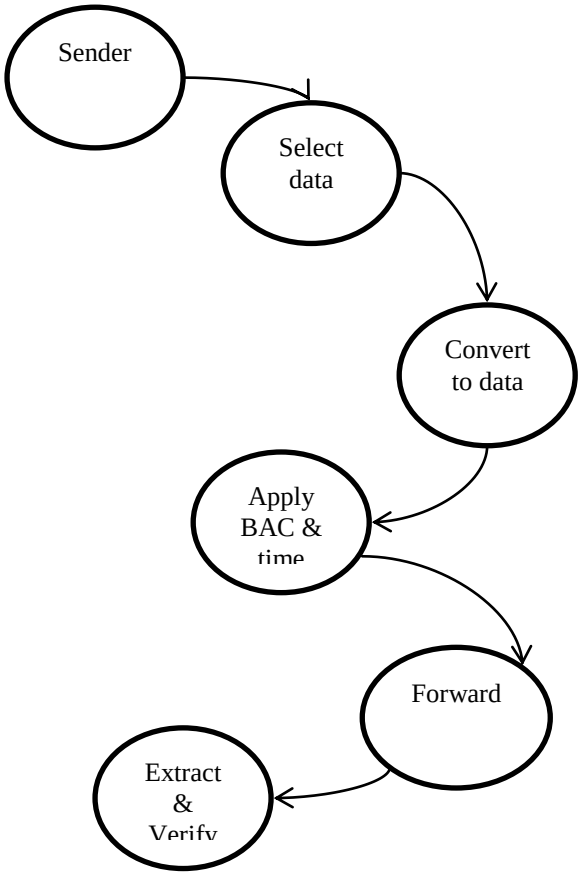
- **BAC Authentication**

With the extracted BAC bits and received data packets, the receiver applies the same hash function (H) on the received data packets with the same secret key (k) to generate the content-based BAC following the same procedure used for BAC generation at the sender side. Then, the extracted BAC is compared with the generated BAC.The comparisons consist of two parts: the first part is on the first n bits, while the second is on the rest f 0 bits.

- **Comparison Graph**

The performance analysis of the existing and proposed work is examined through graphical analysis. Compare the time, throughput and packet delivery ratio.

Extract and Verify The Packets



First users select the data to send a particular person or receiver; then forwarding contents are converted into packets. After converting the packets, applying BAC operations. First step of the BAC is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Second step is to embed the BAC, by adjusting the inter-packet delay. Forward the packets to the receiver. Third step is BAC authentication the receiver applies the same hash function (H) on the received data packets with the same secret key (k) to generate the content.

4. CONCLUSION

In the proposed work a new scheme by adjusting packet timing (delay) to authenticate the data stream. Thus, authentication is done without changing the original packet content and without sending additional authentication information. Extensive experiments are conducted locally and over the Internet based on an implemented prototype system and show that our scheme is robust and practical.

5. FUTURE WORK

In this project proposed a new scheme it is applicable for uni-cast only. In future can extend the work for multicast and broadcast.

REFERENCES

[1] S. Jiang, Y. Liu, Y. Jiang, and Q. Yin, Provisioning of Adaptability to Variable Topologies for Routing mSchemes in MANETs,‖ IEEE J.Selected Areas in Comm., vol. 22, no. 7,pp. 1347-1356, Sept. 2004.

[2] G. Chakrabarti and S. Kulkarni, Load Balancing and in Mobile Ad Hoc Networks,‖ Ad Hoc Networks, vol. 4,pp. 186-203, 2006.

[3] Z. Shen and J.P. Thomas, Security and QoS Self-Optimization inMobile Ad Hoc Networks,‖ IEEE Trans. Mobile Computing, vol. 7,pp. 1138-1151, Sept. 2008.

[4] S. Ibrahim, K. Sadek, W. Su, and R. Liu, Cooperative Communications with Relay-Selection: When to Cooperate and Whom to Cooperate With?‖ IEEE Trans. Wireless Comm., vol. 7, no. 7,pp. 2814-2827, July 2008.

[5] A. Bletsas, A. Khisti, D.P. Reed, and A. Lippman, ―A Simple Cooperative Diversity Method Based on Network Path Selection,‖ IEEE J. Selected Areas in Comm., vol. 24, no. 3, pp. 659-672, Mar.2006.

[6] J. Cai, X. Shen, J.W. Mark, and A.S. Alfa, Semi-Distributed User Relaying Algorithm for Amplify-and-Forward Wireless Relay Networks,‖ IEEE Trans. Wireless Comm., vol. 7, no. 4, pp. 1348-1357, Apr. 2008.

[7] L. Feeney, B. Cetin, D. Hollos, M. Kubisch, S. Mengesha, and H.Karl, Multi-Rate Relaying for Performance Improvement inIEEE 802.11 WLANS,‖ Proc. Fifth Int'l Conf. Wired/Wireless Internet Comm., 2007.

[8] D. Lin and R. Morris, Dynamics of Random Early Detection, ‖Proc. ACM Special Interest Group Data Comm (SIGCOMM),1997.

[9] E. Zohar, I. Cidon, and O. Mokryn, The Power of Prediction: Cloud Bandwidth and Cost Reduction,‖ Proc. ACM Special Interest Group Data Comm. (SIGCOMM), 2011.

[10] V. Venkataramanan, X. Lin, L. Ying, and S. Shakkottai, ―On Scheduling for Minimizing End-to-End Buffer Usage over Multi-Hop Wireless Networks,‖ Proc. IEEE INFOCOM, 2010.

[11] A. Parekh and R. Gallager, A Generalized Processor Sharing Approach to Flow Control,‖ Proc. IEEE INFOCOM, 1992.

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

[13] D.B. Johnson and D.A. Maltz, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, vol. 353, pp. 153-181, 1996.