IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 2 (Jan. - Feb. 2013), PP 56-60
www.iosrjournals.org

A Comparison for Secured Transmission of Packets in Wireless LAN Using AES and ECC

Priyadharshini.K[1], Rajasekar.S.S[2]
[1](PG scholar/CSE, Bannari Amman Institute of Technology, India)
[2](Assistant Professor/CSE, Bannari Amman Institute of Technology, India)

Abstract: *Wireless local area network (WLAN) has increased rapidly, providing flexibility and mobility to the device users. This made the technology popular amongst a wide range of users in the universe. But one of the common problems we are overcoming is fragment loss. So far we were following a scheme to retransmit the entire packet if any fragment is lost. Here we introduce a new scheme called Aggregation with Fragment Retransmission (AFR). In this method, multiple packets are aggregated and transmitted in a single large frame reducing the access overheads and hence increasing the data rate. In addition, to investigate the performance added value when each large frame is fragmented so in the case of error in data frame, only the erroneous fragments are to be retransmitted reducing the error control overheads and this decreases the frame error rate without requiring more overhead.*

The advanced encryption standard is incorporated into existing aggregation method for 802.11 wireless LANs to achieve secure transmission of frames and compute the maximum throughput, optimal frame, and fragment sizes. The proposed system uses weighted fair scheduling with Advanced Encryption Standard (AES) for obtaining optimal fragment size and also used Elliptical curve cryptography (ECC) instead of AES to show that it will reduce the packet size which will be better than AES. We show that our proposed show increase in average rate of successful message delivery over a communication channel and increase in throughput.
Keywords *- 802.11 wireless LAN, AES, weighted fair scheduling, Fragmentation, security overhead*.

I. INTRODUCTION

A wireless network is a type of computer networks that utilizes wireless communication technologies to maintain connectivity and exchange messages between stations over wireless media, such as infrared, laser, radio waves, and ultrasound. Due to the wireless nature, wireless networks possess many advantages against its wired counterpart, for example, capable of device mobility, simple installation, and ease of deployment. Depending on the coverage, wireless networks can in general be divided into five different categories, including wireless regional area networks (WRANs), wireless wide area networks (WWANs), wireless metropolitan area networks (WMANs), wireless personal area networks (WPANs), and wireless local area networks (WLANs). The IEEE standards association establishes five standard series of IEEE 802.22, 802.20, 802.16, 802.11, and 802.15 for the corresponding networks. Among these wireless standard series, the IEEE 802.11 standard is considered the well adopted suite for WLANs due to its remarkable success in both design and deployment.

One of the main challenges in wireless LANs (WLANs) nowadays is to develop a medium access control (MAC) layer that will not decrease the efficiency of the MAC layer when physical (PHY) rates are increased; a theoretical throughput upper limit exists, indicating that by simply increasing the data rate without decreasing overhead, the enhanced performance, in terms of delay and throughput, is bounded even when the data rate goes into infinitely high. Of the existing models, it is particularly concentrated in Aggregation with Fragment Retransmission (AFR) scheme, which was initially proposed in the IEEE 802.11n task group. In this work, multiple frames are aggregated into a larger frame before being transmitted to the physical layer (PHY). If the size of a frame is larger than a pre-established threshold, before aggregation the fragments are made from the frame by dividing it. Transmission errors are handled by retransmitting only the fragments of the frame that had been corrupted [1].

However, the previous work does not consider security, i.e., encryption algorithm AES, which is used in IEEE 802.11i. In other words, when IEEE 802.11n and IEEE 802.11i are both adopted, AES over the high speed wireless LANs (WLANs) must be considered. Analyze the overhead introduced by AES, when added to the aggregation scheme. Compute the optimal frame and fragment sizes which render the maximum throughput in this context, and compare the results to the optimal values, where AES encryption is not used. Derive asymptotic results related to the MAC layer efficiency, expected frame size and saturation throughput. Adding security overhead analysis study is very important due to the importance of security as well as the fact that among the current huge number of papers about IEEE 802.11 performance analysis, none of them considers AES overhead in their analysis. The importance of this paper is therefore partially due to the importance of the security.

Partial packet recovery approaches attempt to repair corrupt packets instead of retransmitting them. Packet recovery relies on the observation that packets with errors may have only a few, localized errors, or at least some salvageable, correct content. Various approaches have been proposed: some rely on physical layer information to identify likely corrupt symbols (related groups of bits) to be retransmitted [10], while others embed block checksums into oversized frames to allow the receiver to recognize partially correct transmissions [9]. Some avoid explicit knowledge and adaptively transmit forward error correction information that is likely to be sufficient to repair bit errors. These approaches have found substantial potential in partial packet recovery, particularly when auto-rate selection mechanisms, which dynamically change the transmission rate to maximize throughput without too many errors, may choose too high a rate, thus creating errored packets to be recovered.

II. FRAGMENT ENCRYPTION

Packets are fragmented into small packets because large packets are difficult to send. After fragmentation, if encryption is needed (i.e., AES is used), each fragment needs encryption. In other words, if a large frame is divided into multiple fragments, the system needs to spend time encrypting each fragment before transmitting it, and decrypting each fragment after receiving it, respectively. Such encryption/decryption introduces more overhead in terms of time.

A. Dynamic Weighted Fair Scheduling

In this section we present the proposed algorithm to improve QoS in WLAN namely, Dynamic Weighted Fair Scheduling Scheme (DWFSS). We introduce a new dynamic weight adjustment algorithm to provide fairness and increase bandwidth utilization. A new scheduling algorithm which can provide differentiated services to both high and low priority traffic is also presented. Based on the literature review it is understood that the SS [6] is unable to provide bandwidth guarantees. The SS shows poor performance in terms of fairness and is unable to prevent starvation. The main reason for this poor performance is due to the first-come first-serve (FCFS) admission control algorithm [8]. In the FCFS mechanism, any flows requesting for bandwidth will be granted the requesting bandwidth until the bandwidth is fully exhausted.

In FCFS algorithms the bandwidth and medium access rate is only determined by the order of arrival. When the bandwidth is exhausted the scheduler starts to reject new flows until some of the admitted flows complete their transmission. Hence this causes unfairness and starvation to the traffic arriving later. Thus, a dynamic bandwidth management mechanism is needed to solve this unfairness problem in WLAN. In order to overcome the unfairness problems faced by the standard scheduler we propose a new algorithm, the DWFSS. The purpose of this algorithm is to provide bandwidth reservation and fairness during admission control. The DWFSS defines functionalities to dynamically allocate bandwidth to different types of traffic. The DWFSS will be able to differentiate traffic based on the priority of traffic and provide services based on the requirements of each flow. DWFSS is also a low overhead algorithm as it uses the same simple algorithm for both static and mobile nodes.

B. Advanced Encryption Standard

Advanced Encryption Standard (AES) algorithm consists of four stages that make up a round which is iterated 10 times for a 128-bit length key, and 14 times for a 256-bit key. The first stage "Sub Bytes" transformation is a non-linear byte substitution for each byte of the block. The second stage "Shift Rows" transformation cyclically shifts (permutes) the bytes within the block. The third stage "Mix Columns" transformation groups 4-bytes together forming 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1). The fourth stage "AddRoundKey" transformation adds the round key with the block of data. In this structure, some of the bits of the intermediate state are transposed unchanged to another position. AES does not have a structure of Feistel but is composed of three distinct invertible transforms based on the Wide Trial Strategy design method.

For Security purpose encryption is needed (i.e., AES is used), each fragment needs encryption. In other words, if a large frame is divided into multiple fragments, the system needs to spend time encrypting each fragment before transmitting it, and decrypting each fragment after receiving it.

C. Integrate a Weighted Fair Scheduling with AES

There has also been work on distributed protocols that takes priorities into account when performing medium access control. For instance, Aad and Castelluccia [1] present service differentiation mechanisms for wireless network and their mechanism allows a host to pick a backoff interval as a function of its priority, intervals of larger backoff being used for lower priority. Our proposed method is weighted fair scheduling mechanism which uses a similar mechanism, but our goal is to achieve weighted fair scheduling, not priority scheduling. The objective behind this work was to develop a fair scheduling MAC protocol for a wireless LAN with the following properties:

i) The protocol must be fully distributed in that no single node should have any special responsibility.
ii) Each node should be able to independently determine when to transmit a packet, without knowing the state of (or existence of) flows at other nodes—the state of a flow includes information such as flow's weight, even when the flow is backlogged or not, and the packets on the flow arrival time.
iii) Maintain compatibility or close resemblance to an existing wireless MAC standard, to implement the proposed protocol and make it easier.

AES is integrated with dynamic weighted fair scheduling.

D. Integrate a Weighted Fair Scheduling with ECC

The second protocol is ECC, the Diffie-Hellman key agreement based on Elliptic Curve Cryptography (ECC) which does not need any trusted third party. In its standard form, ECC does not provide authentication. The two parties A and B must possess a certificate generated by an authority.

They agree to use the same curve parameters and generate in advance their private keys, kA and kB and public keys QA = kA _G and QB = kB _G where G is the generator of the group defined by the elliptic curve. In this protocol, A and B first exchange random nonces. Then, B sends its certificate to A (its public key signed by the authority using ECDSA). After the certificate verification, A uses his private key and B's public key to perform a point multiplication and arrive to a common secret kA fi kB fi G, which is used with the exchanged nonces to derive a shared secret key. Then, A sends its certificate to B who performs the same operations to obtain the shared secret (kA fi kB fi G = kB fi kA fi G) and derive the shared secret key. The possession of the shared secret key is proved in the ability of both parties to encrypt the exchanged nonces and their identities with the shared secret key.

III. FRAGMENT AGGREGATION

Packets are aggregated into a single large frame because transmitting must not take much time so in order to reduce transmission time we aggregate them into single large frame. We perform a mechanism to aggregate these packets which are coming from upper layer.

Aggregation schemes seek to amortize the PHY header overhead across multiple packets. This is achieved by transmitting multiple packets in a single large frame. However, there is a traditional dislike for transmitting large frames in wireless networks since in a noisy channel the throughput can fall as larger frames are used.Here for aggregation we use zero waiting mechanism. The main idea of the AFR scheme is to aggregate several packets received at Mac level from the upper layer into one large frame [7]. The algorithm defines also a fragmentation threshold where the packets whose size exceeds that fragmentation threshold are divided into fragments.

Considering the AFR scheme, there is two possibilities of errors:

1. Data frame is corrupted while the ACK message is received correctly. In this case, AFR scheme uses at the sender side the ACK bitmap to inform the sender about the corrupted fragments of the frame. This case of AFR errors is considered as a successful transmission.
2. The loss of the ACK message is considered as a collision. In this case, AFR behaves similarly to DCF in case of collision.

A. Optimal Fragment Size

Fragmentation plays a central role in aggregation schemes such as AFR, with fragments being the unit used for retransmission. When a very small fragment size is used, only corrupted bits are retransmitted but since each fragment has a fixed size header the overhead is large. When fragment size is large, the overhead created by the fragment header is small but many bits will be unnecessarily retransmitted since a single damaged bit in a fragment will lead to the entire fragment being retransmitted. For a given BER there therefore exists an optimal fragment size that balances the tradeoff between fragment header overhead and excessive retransmission. We consider throughput versus fragment size from which the existence of an optimal fragment size that maximizes throughput is evident. Observe that the optimal fragment size depends on the BER, as is to be expected (128, 512 and 1024 bytes for BER=10−4, 10−5, 10−6 respectively).

In practice, we are interested in determining a simple scheme that approximates the optimal fragment sizes performance. It can be seen from results that the throughput peak is relatively flat and broad and thus we expect that the throughput reduction resulting from an approximate scheme can be kept relatively small. The reduction in throughput, compared to that achieved with the optimal fragment sizes, of using a sub-optimal fragment size. From result we can see that if we can tolerate a throughput loss of up to 10%, then fragment sizes of 128 bytes and 256 bytes are near optimal across a wide range of BERs. It can be seen that fragment sizes of 128 and 256 bytes are always able to achieve within 10% of the maximum possible throughput. We have

obtained similar results under a wide range of conditions including different numbers of stations, but these are not included here due to their similarity to the results.

B. Identifying Corrupted Fragment

At the receiver end after receiving the frame we perform a operation in order to identify the corrupted fragments. Each fragment header is composed of six fields: packet ID (pID), packet length (pLEN), startPos, offset, spare, and FCS. pID and pLEN represent the corresponding ID and length of the packet P to which this fragment belongs. startPos is used to indicate the position of the fragment body in this frame, and offset is used to record the position of this fragment in packet P. The new ACK format is simple; we add a 32-B bitmap to the legacy ACK format. Each bit in the bitmap is used to represent the correctness of a fragment.

C. Retransmission Mechanism

When the channel is lightly loaded to the extent that the DCF is enough, deliberate waiting only leads to higher delays. If the channel is in a heavily loaded condition where backlogged buffers mean the desired numbers of packets to form large frames are always available when transmission opportunities are won, then all waiting schemes are the same. If the channel is in an intermediate situation between these two extremes, waiting for a certain amount of time for packets to accumulate seems reasonable at first glance. Nevertheless, we argue that fundamentally there is no need to wait for packets to accumulate at the MAC layer, and it is sufficient to start a transmission whenever the MAC wins a transmission opportunity.

This batch retransmission mechanism evidently performs well in both lightly and heavily loaded situations. In the intermediate state, the frame size used adapts to the minimum required to service the offered load. Specifically, when the current level of efficiency is too low for the offered load, a queue backlog will develop which in turn induces larger frames and increased efficiency. If the incoming traffic subsides, smaller frame sizes will be automatically selected. Evidently, such a policy minimizes holding delay at the MAC layer.

IV. RESULT AND DISCUSSION

Network Simulator ns2 is used for simulations. The terrain size consists of the 16 number of the mobile ad-hoc nodes that can randomly placed in a terrain area size of 1000 m×1000m.Here we consider the maximum wireless channel capacity is considered to be 2 Mb/s. Each of the simulations is performed for a simulation time of 50 seconds set. Selfish aware queue management mechanisms are applied for varying number of the selfish nodes. A Simple priority algorithm is compared with existing under the simulated conditions. The data sources for each node are considered to be in Constant Bit Rate. Each of the source nodes transmits packets at a certain rate. The performance of the network is analyzed by varying the Packet size.

We compare the computational overhead of the proposed protocol with AES and ECC. The measurement of computational overhead is in terms of number of energy intensive operations such as scalar multiplications, signature generation and verification used in the protocols.

Table.1

Algorithm	Packet size before encryption	Packet size after encryption
ECC with AFR	500 bytes	587 bytes
AES with AFR	545 bytes	614 bytes

V. CONCLUSION

The advanced encryption standard is incorporated into existing aggregation schemes for in order to obtain secure transmission of frames and compute the optimal frame, maximum throughput, and fragment sizes which can be achieved in this context and compare them to the optimal values when encryption is not used. Dynamic weighted fair scheduling is used in order to avoid problems due to large aggregated frame. Also evaluate the delay performance of such a scheme in the context of encryption and study asymptotic properties of the medium access control layer efficiency, throughput, and expected frame size.

Problems in existing system are Existence of AES in fragment doubles optimal fragment size. Huge aggregated frame causes problem so we have to reduce the frame size. We also found that by using ECC packet size will be reduced. Our future work is to use weighted fair scheduling and Hyper elliptical curve which will reduce key size than ECC which alternatively reduces fragment size.

REFERENCES

[1] J. Tourrilhes, "Packet frame grouping: improving IP multimedia performance over CSMA/CA," in *Proc. ICUPC*, 1998, pp. 1345-1349.

[2] B. Sadeghi, V. Kanodia, A. Sabharwal, and E. Knightly, "Opportunistic media access for multirate ad hoc networks," in *Proc. ACM MOBICOM*, 2002, pp. 24-35.

[3] Y. Xiao and J. Rosdahl, "Throughput and delay limits of IEEE 802.11,"*IEEE Commun. Lett.*, vol. 6, no. 8, Aug. 2002, pp. 355-357.

[4] Y. Xiao and J. Rosdahl, "Performance analysis and enhancement for the current and future IEEE 802.11 MAC protocols," *ACM SIGMOBILE Mobile Computing Commun. Review*, vol. 7, no. 2, pp. 6-19, Apr. 2003.

[5] Q. Ni, I. Aad, C. Barakat, and T. Turletti, "Modeling and analysis of slow CW decrease for IEEE 802.11 WLAN," in *Proc. PIMRC*, 2003, pp. 1717-1721.

[6] Q. Ni, T. Li, T. Turletti, and Y. Xiao, "AFR partial MAC proposal for IEEE 802.11n," IEEE 802.11-04-0950-00-000n, Aug. 2004.

[7] V. Vitsas, *et al.*, "Enhancing performance of the IEEE 802.11 distributed coordination function via packet bursting," in *Proc. GLOBECOM*, 2004, pp. 245-252.

[8] C. H. Foh and J. W. Tantra, "Comments on IEEE 802.11 saturation throughput analysis with freezing of backoff counters," *IEEE Commun. Lett.*, vol. 9, no. 2, pp. 130-132, Feb. 2005.

[9] J. Choi, J. Yoo, S. Choi, and C. Kim, "EBA: an enhancement of the IEEE 802.11 DCF via distributed reservation," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 378-390, July 2005.

[10] T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, and T. Turletti,"A new MAC scheme for very high-speed WLANs," in *Proc. IEEE WOWMOM*, 2006, pp. 171-180.

[11] X. Yang and N. Vaidya, "A wireless MAC protocol using implicit pipelining," *IEEE Trans. Mobile Comput.*, vol 5, no. 3, pp. 258-273, Mar. 2006.

[12] Y. Xiao, H. Li, K. Wu, K. K. Leung, and Q. Ni, "On optimizing backoff counter reservation and classifying stations for the IEEE 802.11 distributed wireless LANs," *IEEE Trans. Parallel Distributed Syst.*, vol. 17, no. 7, pp. 713-722, July 2006.

[13] T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, and T. Turletti, "Aggregation with fragment retransmission for very high-speed WLANs," *IEEE/ACM Trans. Networking*, vol. 17, no. 2, pp.591-604, Apr. 2009.

[14] High-Speed Wireless 802.11 LANs," *IEEE Trans. wireless communications*, vol. 9, no. 1, pp. 218-226, January 2010.

[15] N.Khan, M.G.Martini, Z.Bharucha, and G.Auer," Opportunistic packet loss fair scheduling for delay-sensitive applications over LTE systems" Wireless Communications and Networking Conference, pp.1456-1461,April 2012.

Bibliography

Ms. K.Priyadharshini received her B.E IT from Avinashilingam University for women, Coimbatore, India and she is now pursuing her M.E in Computer Science & Engineering at Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India. She had participated in Various National Level Technical Symposium held at Various Engineering Colleges in Tamil Nadu .She had published 2 Papers in Various National and International Conferences held at Engineering Colleges. She had attended workshops and seminars in diverse disciplines held at various Engineering Colleges.

Prof. Mr.S.S,Rajasekar received his M.Sc in Software Engineering , he also received his M.E in Computer Science and Engineering and now he is pursuing his Ph.D. in Wireless Networks at Anna University of Technology, Coimbatore. He is currently working as Assistant Professor in the department of Computer Science and Engineering, Bannari Amman Institute of Tech, Sathyamangalam, Erode, TamilNadu, India. He has 2 years of experience in teaching field. He has published paper in International Conference. He has attended various workshops, conferences and staff development program held at various reputed engineering colleges.