Advances in Engineering Research (AER), volume 153
2017 International Conference Advanced Engineering and Technology Research (AETR 2017)

CSMA/CA Analysis Based on the Markov Chain

Wei Wang[1, a *] and Wenhong Zhao[2,b]

[1] Science and Technology on Communication Information Security Control Laboratory, Jiaxing Zhejiang 314001, China

[2] Nanhu College, Jiaxing College, Jiaxing 314001, China

[a]wwzwh@163.com, [b]whzhaonh@163.com

Keywords: Markov chain; CSMA/CA; MAC; Network security

Abstract. First, the CSMA/CA mechanism is modeled. Then, based on markov chain theory, the attack method of CSMA/CA is analyzed from two aspects of stochastic performance model and bandwidth sharing model. After discussing the typical attack methods, through the throughput, communication efficiency and collision number analysis the performance of attack methods, verified the CSMA/CA based on the theory of markov chain vulnerability analysis method is feasible and effective. Finally, this paper presents a simple and efficient MAC protocol for full duplex network - full duplex MAC protocol.

Introduction

Attack to wireless communication networks is of great significance for the research of network security. Many researchers have made a lot of relevant research [1-9]. Due to the characteristics of self-organization, multi-node, high-bandwidth and burst communications of the future wireless networks, the application of fixed multiple access technologies may be limited, such as FDMA, TDMA, etc. However, dynamic multiple access technology of ALOHA mechanism is not applicable to wireless networks due to its throughput. Thus, CSMA/CA mechanism will be subject to more and more attention from wireless network researchers because of its timeliness, scalability, support for burst communications, prevention of hidden terminal/exposed terminal, etc. Zhang Junyi discussed the intelligent lamming attack and deception jamming in single-node and multi-node collaborative methods to Ad Hoc networks based on MAC protocol and compared the interference effects of different ways [5]. [10-12] Attack is realized by periodic transmission of RTS and CTS frames by the violated node forging NAV value. Such attack results in that the nodes within one hope of the violated node wrongly update the local NAV value according NAV value field in RTS and CTS frames and mistake the channel is busy, which increases the delay of access to the channel. Zeng Hongyi et al proposed an attack model on CSMA/CA, analyzed the effectiveness and impact of the attack mode through the associated network simulation and data processing, proposed an evaluation standard for the efficiency of network attacks, and finally analyzed the improvement of the attack methods and random backoff algorithm [13]. Cao Chunjie et al proposed a RTS-CTS attack on IEEE 802.11 CSMA/CA, wherein the attacker preempts the traffic channel by modifying the contention window. This attack can keep the target workstation or network access point silent and even cause the network paralysis [14].

The above discusses the possibility of attacks on CSMA mechanism from the technical aspect but it still needs further theoretical analysis. This paper focuses on research of CSMA/CA channel access mechanism and discusses the attack methods on CSMA/CA channel access mechanism through theoretical analysis and study. This paper also proposes a new full-duplex MAC (FD-MAC) and analyzes the performance of Full duplex communication network based on FD-MAC protocol.

Feasibility analysis of CSMA/CA access attack

RTS and CTS are CSMA/CA control frameworks for specifying the next channel slot. Before sending actual data frames, exchanging the RTS and CTS is one of the main channel reservation method, it can solve the hidden terminal and exposed terminal problem ", at the same time can also be sent via basic

CSMA/CA access method at the same time large amounts of data. RTS and CTS frames contain time fields, defining data frames and ACK channels to take up time. All workstations within the coverage of the source and destination stations will receive moderate booking information. The implementation is as follows: send node listening channel. If the channel has free contiguous DIFS (interframe space between distributed coordination functions), it will send RTS frames. Otherwise, it will activate the binary exponential inversion algorithm in the current and subsequent DIFS. When RTS is received, the target node will send the CTS after a SIFS (short frame space). After receiving CTS, the source station can send data frames after a SIFS; After the target station receives the data frame, it can send the ACK frame after a SIFS; After receiving the ACK frame at the source, the data transfer is confirmed as successful. All other stations listening to RTS and CTS frames update their navigation (network assignment vector) values through the duration fields of RTS and CTS frames, and remain silent during that time. The duration field value of RTS frames is the sum of CTS frame time, data frame transfer time, ACK frame time, and three SIFS. The CTS frame duration field is the sum of data transfer time, ACK frame, and two SIFS. All nodes will compete again after the net asset value (i.e.,) is over. The data transmission is over. Fig 1. shows the schematic diagram of the RTS - CTS handshake. The above DIFS and SIFS are composed of multiple slots.

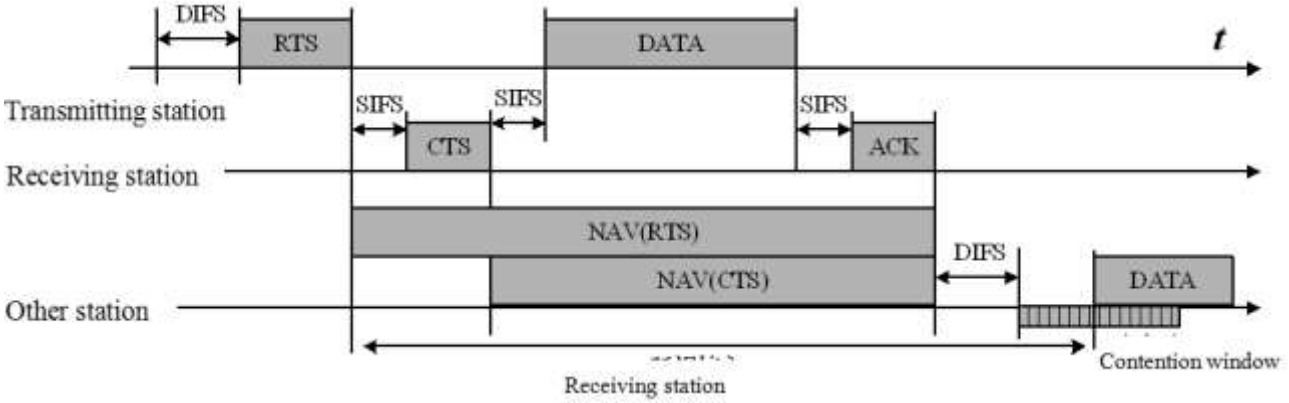

Figure 1. RTS-CTS handshake

During the communication process, the work node will hog the channel through RTS and CTS until the data transfer is complete. Assume the attacker has the location and function of the control frame "type" and "duration" fields, as shown in Fig. 2. In the channel reservation process, the value of the navigation is recorded using the "duration" field, and the time for the communication between the two parties to access the wireless media is specified by the NAV. Therefore, attackers can attack this mechanism in this way, thus occupying the channel, preventing the workstation data transmission, and even blocking the network access points and disabling the entire wireless network.

Unknown	Type	Unknown	Duration	Unknown

Figure 2. Channel access control frame only mastering duration field

Attacker attacks: attacks can be done in a variety of ways that can be targeted at network access points, mobile terminal nodes, or both. An attacker needs to listen for network traffic data to navigate synchronization. In addition, this attack method can only be achieved by RTS or RTS - CTS. The main attack methods are as follows:

Against one or more nodes, as shown in Fig. 3, the attacker intercepts the RTS frame and modify the "duration" field according to the "type" field, and then send an RTS frame target node notification data is transmitted in the current wireless network executive compensation process, so that the target node in a certain period of time can't transmit data. The attack node performs a normal callback procedure with no abnormal behavior. Because of the failure of receiving RTS frames, other nodes can communicate

normally. In general, network communication is normal. This attack is not easy to detect and can provide further wireless injection attacks for target nodes.

Attack access points: as shown in Fig. 4, wireless network access points and other network nodes compete for the same common channel. As a result, the RTS framework with the modified "duration" field may have an aversion to network access points to perform the fallback process. During an attack, the network access point cannot send data so that it cannot respond to requests from all nodes. Therefore, all nodes are automatically disconnected from the network access point, thus making the entire network unable to communicate.

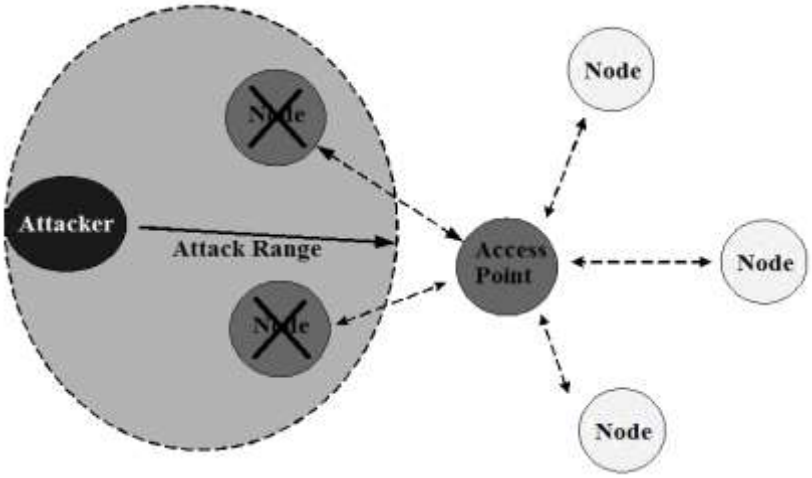

Figure 3. Attacks to nodes

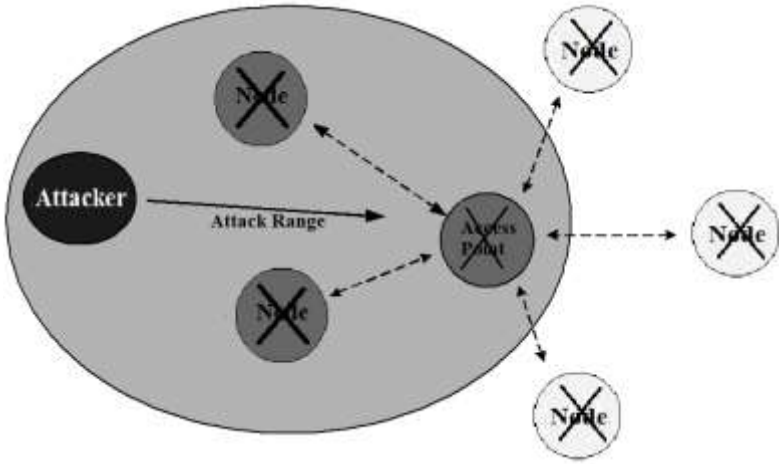

Figure 4. Attacks to the network access point

The probability that an attacker can successfully preempt the channel is: the minimum channel contention window is set to the CW, and the network node number is n, the maximum retransmission time of frame to r. Network nodes are in binary exponential backward mechanism. The attacker always selects the No. 0 contention window. Therefore, only the first node that conflicts with an attacker may suffer a second collision. After the first frame, the attacker will send the second frame immediately. Therefore, the NAV of the node that did not collide for the first time will not be reduced by 1 for the second frame, and only the nodes of the first collision can select the No. 0 window at random.

From the RTS - CTS mechanism, once the attacker preempts the channel, the subsequent frames will be sent in SIFS, while the other network nodes won't be able to access the channel. Then, the probability that the attacker successfully grabs the channel within a frame's transmission cycle ($Pr_{success}$) is shown below.

$$\Pr_{success} = 1 - \Pr_{fail}; \Pr_{fail} = \Pr_{fail,r};$$

$$\Pr_{fail,r} = \frac{1}{2^{r-2}} \Pr_{fail,r-1} \cdot \left(1 - \left(\frac{2^{r-2} CW - 1}{2^{r-2} CW} \right)^n \right);$$

$$\Pr_{fail,1} = 1 - \left(\frac{CW - 1}{CW} \right)^n$$

FD - MAC protocol

This section describes the detailed flow of the FD-MAC protocol proposed in this article. The FD-MAC protocol is based on the IEEE802.11 RTS/CTS protocol, which is compatible with the IEEE802.11 protocol and can fully utilize the advantages of full-duplex wireless. Fig. 5 is the main process of packet transmission in the fd-mac protocol.

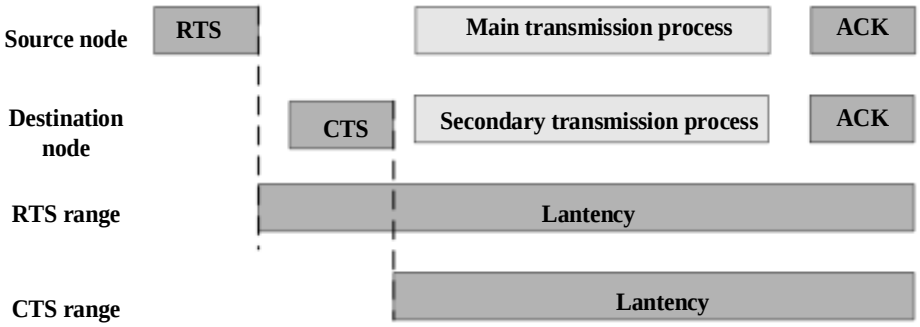

Figure 5. Packet switching process

As shown in Fig. 5, the source node USES the standard RTS/CTS protocol when the source node is to send the packet to the destination node. The source node listens for the channel at regular intervals, which is called distributed inter frame space (DIFS). When the channel is idle within DIFS interval, the source node opens the random withdrawal counter, and the size of the withdrawal counter is selected randomly according to the competition window. When the withdrawal counter terminates, the source node sends the RTS group to the destination node. Once the RTS grouping is received, the destination node returns the CTS group to the source node. When other nodes in the network receive RTS or CTS groups, the delay packet is sent until the current packet transmission is over. Fig. 6 shows the reservation area when the source destination node group is transferred.

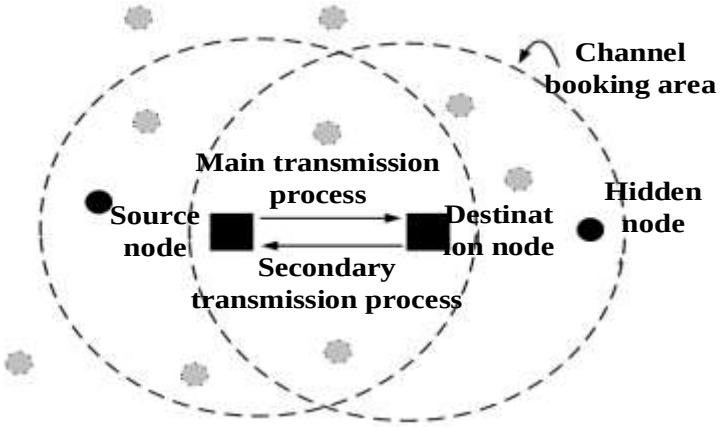

Figure 6. FD-MAC Channel booking area

When RTS/CTS is exchanged, the data packets are transferred from the source node to the destination node. We call this packet transmission as the primary packet transmission. During the main packet transmission, the receiver can transmit the packet to the transmitter node at the same time, known as the secondary packet transmission. Because the channel is reserved for primary packet transmission in the process of sending packets to the destination node in the source node, the subgroup transfer does not need to reserve the channel through the additional RTS/CTS grouping. The main transmitter and the secondary transmitter both send ACK confirmation packets at the end of the main packet transmission, even if the subgroup is terminated earlier than the main packet transmission. In order to improve the decoding efficiency of the control packet transmission, this paper USES the fixed transmission rate to send the control group. When the RTS groups of different nodes collide, the destination node cannot decode the RTS grouping correctly.

Experimental Results and Analysis

Fig. 7 shows the throughput simulation results of FD-MAC and conventional schemes with the change of transmission power. The main parameters are: the node density is 0.00001 nodes/m^2, the spacing of the two nodes is 100 meters.

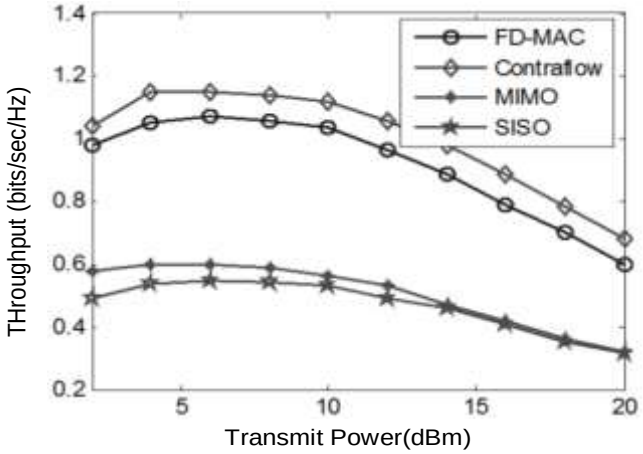

Figure 7. Throughput VS launch power simulation results of different systems

Although the throughput of the FD-MAC protocol is less than the Contraflow protocol, the throughput gap is small. This is mainly due to the fact that fd-mac requires additional control packet RTS/CTS grouping costs to take up a certain throughput. Here, it is known that full duplex system are more significant than half duplex system throughput advantage, since full-duplex communication system needs only a channel will be able to complete the bidirectional data packet transmission, half duplex system requires two channel. When packet transmission conflict Contraflow agreements caused by discarding the transmission group resource waste, but because of the packet transmission rate is greater than the MAC control packet transmission rate, which produce high throughput performance. Furthermore, according to Fig. 7, the transmitting power of the system with the maximum throughput is not the maximum and not the minimum emission power. When considering both physical and MAC layers, low emission power can be used to lower the packet transmission rate, and high emission power will result in MAC competition cost and interference increase. When the optimal emission power is obtained, the maximum throughput can be obtained when the physical and MAC layers are in balance.

Fig. 4 shows the simulation results of energy consumption of different systems with emission power changes.

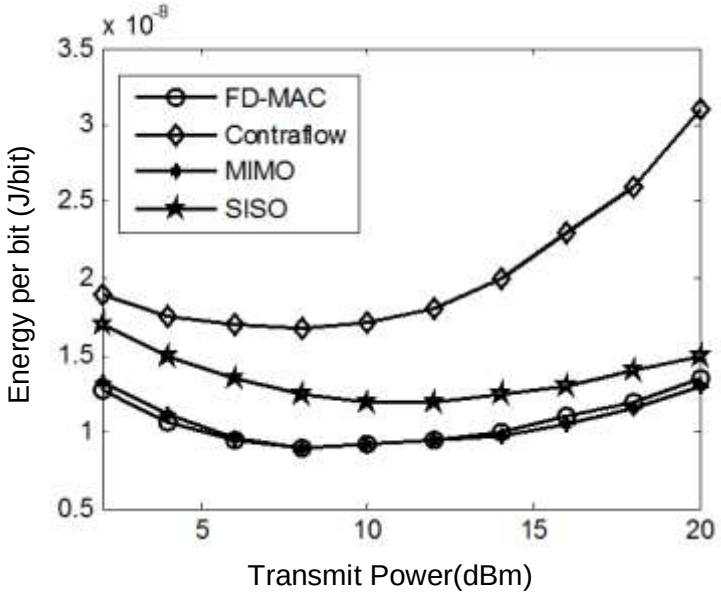

Figure 8. Simulation results of energy consumption VS emission power of different systems

According to the figure, the FD - MAC protocol and half duplex MIMO network with minimal energy consumption, which under the condition of low transmission power FD - MAC has smaller energy consumption, and under the condition of high transmission power MIMO has smaller energy consumption, but the energy consumption difference is small. Under the condition of low transmission power FD - MAC has a better performance this is the same as its energy consumption has a smaller MAC overhead, whereas multi-input multi-output (MIMO) energy consumption under the condition of high transmission power performance is better is it because of its under the condition of high transmission power is higher than full-duplex communication throughput performance. Contraflow has the worst performance because if there is a conflict there is a need to re-transmit the bi-directional data packet, and the secondary group will consume an additional amount of busy signal energy when compared to the main group hour. It is also known that the required emission power required for minimum energy consumption is not the smallest or largest of all communications systems. At low emission power levels, power consumption decreases but the duration of power consumption increases, as well as increases in energy consumption. While high emission power level, packet transmission cycle decreases but power consumption increases. And the MAC layer's energy consumption increases with the launch power. Therefore, when designing optimal energy consumption network, the optimal emission power needs to be selected through numerical evaluation.

Conclusion

In this paper, the CSMA/CA mechanism is formally modeled firstly. Based on the Markov Chain theory, the analysis of attack on CSMA/CA is introduced from two aspects, such as the stochastic performance model and bandwidth share model. Then, the specific attack methods and performance analysis is introduced and the feasibility and effectiveness of attack to CSMA/CA mechanism is verified. The full duplex MAC protocol was proposed. And half duplex system, based on the traditional existing MAC protocols of full duplex system performance comparison, FD - MAC to lower energy consumption under the condition of gain competitive throughput performance, has the very good reference value.

References

[1] Y. Tao, Z.L. Liu, Z.N. Zhang, et. Al,. Research on Network Attack Situation Niching Model Based on FNN Theory; High Technology Letters, 2010, 7:680-684.

[2] Q. Wang, Y.J. Feng, Z.M. Yang, et. al. Network Attack Model Based on Ontology and its Application, Computer Science, 2010, 37 (6):114 -117.

[3] G.Y. Wang, H.M. Wang, Z.J. Chen, et. al. Research on Computer Network Attack Modeling Based on Attack Graph; Journal of National University of Defense Technology, 2009, 31 (4):74-80.
[4] F.F.Zhao, X.Z. Chen, J.H. Li; Generation Methods of Network Attack Graphs Based on Privilege Escalation; Computer Engineering, 2008, 34 (23):158- 160.
[5] J.Y. Zhang; Research on Ad Hoc Network Attack Based MAC Protocol; Radio Engineering, 2008, 38 (10):4 -6.
[6] F. Chen, Y.X. Luo, X.J. Chen, et. al. Progress of Research of Network Attack Technology; Journal of Northwestern University: Natural Science, 2007, 37 (2):208- 212.
[7] J.W. Zhuge, X.H. Han, Z.Y. Ye, et. al.; Network Attack Plan Recognition Algorithm Based on Extended Goal Graph; Chinese Journal of Computers, 2006, 29 (8):1356 -1366.
[8] L. Yu, B. Chen, J.M. Xiao; A Network Attack Path Reconstruction Program; Journal of University of Electronic Science and Technology of China, 2006, 35 (3):392 -395.
[9] Y.G. Zhang, D.X. Li; Analysis of Network Attack and Intrusion under IPv6; Computer Science, 2006, 33 (2):100- 102.
[10]G Noubir, G Lin. Low power DoS attacks in data wireless LANs and counter measures. ACM MOBIHOC, 2003, 26(12): 62-69.
[11]M. Raya, J. E Hubaux and I. Aad. DOMINO: A system to detect greedy misbehavior in ieee 802.11 hotspots. In Proc. Of ACM MobiSys, 2004.
[12]J. Rdouceur. The Sybil Attack. http://research.microsoft.com/sn /Farsite/IPTPS2002.pdf. 2002
[13]H.Y. Zeng, W.Z. Wenzhu, Z.X. Xu, et. al. Research on the IEEE 802.11 MAC Sublayer Attack Mode; Network Security Technology & Application, 2007, 9:39-41.
[14]C.J. Cao, H.W. Yang, W. Wang; RTS-CTS Attack on IEEE 802.11CSMA/CA; Communication Countermeasures; 2009, 4:32-35.