Analysis of Security Vulnerability in Cooperative Communication Networks

Ki Hong Kim
The Attached Institute of ETRI
Daejeon, The Republic of Korea
Email: hong0612@ensec.re.kr

***Abstract*—Cooperative communication is a new and emerging wireless communication that exploits spatial diversity to improve wireless channel capacity. Cooperative medium access control (CoopMAC) protocol is a MAC protocol that involves an intermediate relay between a transmitter and a receiver in the cooperative network. In this paper, we identify various attacks against CoopMAC and analyze security vulnerabilities in CoopMAC. From our analytical results, it can be induced that there is a need for an efficient authentication procedure which provides reliability and security for normal CoopMAC communication. To our knowledge, this is the first comprehensive case study of security vulnerabilities caused by possible security attacks in CoopMAC. Our results can be used to design an efficient and secure communication mechanism for cooperative networks.**

***Keywords*-CoopMAC; cooperative communication; security vulnerability; authentication**

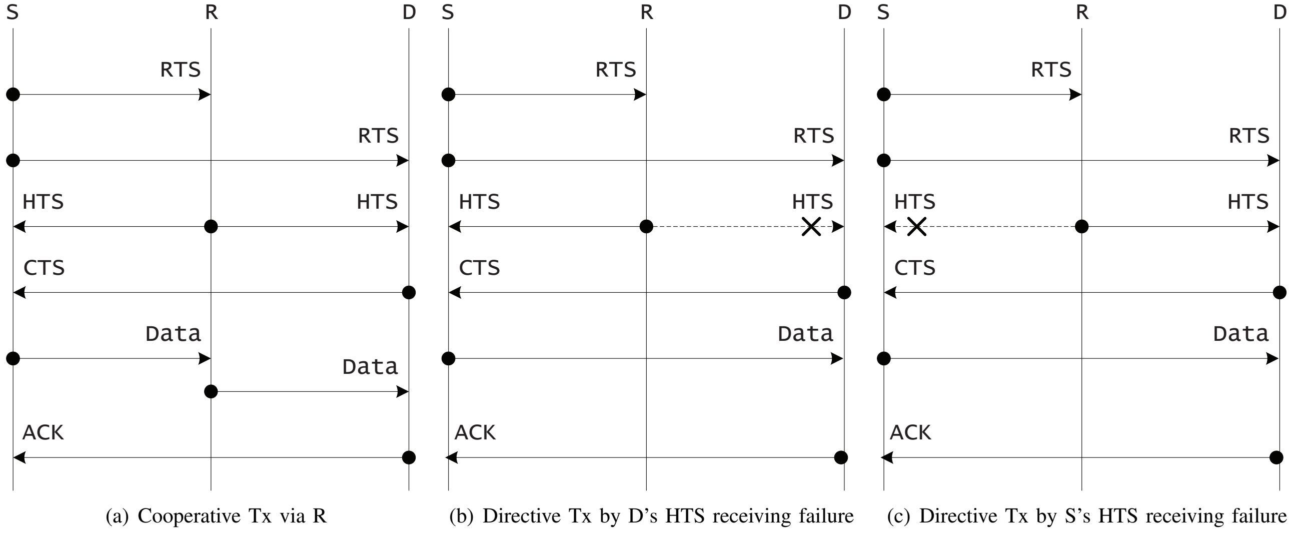
I. Introduction

Cooperative communication is indispensable for making ubiquitous communication connectivity a reality. Cooperative communication is an innovative wireless communication mechanism that takes advantages of the open broadcast nature of the wireless communication channel and the spatial diversity to improve channel capacity, robustness, reliability, delay, and coverage. In the cooperative communication network, when the source node transmits data packet to the destination node, some nodes that are close to source node and destination node can serve as relay nodes by forwarding replicas of the source's data packet. Among the forwarding methods employed by the relay nodes, amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) are the most common methods. The destination node receives multiple data packet from the source node and the relay nodes and then combines them to improve the communication quality [1][2].

A MAC protocol called CoopMAC is designed to improve the performance of the IEEE 802.11 MAC protocol [3] with minimal modification. It is able to increase the transmission throughput and reduce the average data delay. It also utilizes the multiple transmission rate capability of IEEE 802.11b, 1 to 11Mbps, and allows the source node far away from the access point (AP) to transmit at a higher data rate by using a relay node [4][5].

Although cooperative communication has recently gained momentum in the research community, there has been a great deal of concern about cooperative communication mechanism and its security issues. There have been several previous related works regarding communication techniques and security issues for cooperative network. The work in [1][2] described wireless cooperative communication and presented several signaling schemes for cooperative communication. In [4][5], a new MAC protocol for the 802.11 wireless local area network (WLAN), namely CoopMAC, was proposed and its performance was also analyzed. The potential security issues that may arise in a CoopMAC were studied in [6], and various security issues introduced by cooperating in Synergy MAC were also addressed in [7]. The [8] suggested cross-layer malicious relay tracing method to detect signal garbling and to counter attack of signal garbling by compromised relay nodes, while the [9] presented the distributed trust-assisted cooperative transmission mechanism handle relays' misbehavior as well as channel estimation errors. Also, a performance of cooperative communication in the presence of a semi-malicious relay which does not adhere to strategies of cooperation at all time was analyzed in [10], and a statistical detection scheme to mitigate malicious relay behavior in DF cooperative environment was developed [11]. The examination of the physical consequences of a malicious user which exhibits cooperative behavior in a stochastic process was discussed in [12]. The [13] described a security framework for leveraging the security in cognitive radio cooperative networks. However, most of the works on cooperative communication is focused on efficient and reliable transmission schemes using the relay and identification of general security issues caused by the malicious relay node. No work has been done on the analysis of denial of service (DoS) vulnerability caused by an attacked relay node in cooperative communication environments.

In this paper, a cast study of DoS attack in CoopMAC is presented for the first time. Security vulnerabilities at each protocol stage while attacking a cooperative communication, namely between a source node and a relay node, between a relay node and a destination node, and between a source node and a destination node, is analyzed and compared. This study differs from previous works in that it concentrates on one significant aspect of security vulnerability in the CoopMAC, namely DoS vulnerability of CoopMAC caused by the Dos attack of attacker node. This is believed to be the



(a) Cooperative Tx via R (b) Directive Tx by D's HTS receiving failure (c) Directive Tx by S's HTS receiving failure

Figure 1. Control packet exchange in CoopMAC protocol

first comprehensive analysis and comparison of the security vulnerability from possible DoS attack in CoopMAC. The analytical results can be used to design an efficient and secure communication mechanism for cooperative communication security.

The remainder of this paper is organized as follows. In section II, we describe the characteristics of CoopMAC. Next, in section III, we identify some possible security attacks against CoopMAC and then analyze the security vulnerabilities at each protocol stage of CoopMAC. Finally, in section IV, we review our conclusions and detail plans for future work.

II. Overview of CoopMAC Protocol

CoopMAC is a MAC protocol based on the IEEE 802.11. It employs request-to-send (RTS) and clear-to-send (CTS) control packet to establish communication, which are overheard by other nodes besides the source node and the destination node. The CoopMAC is totally compatible with the legacy 802.11 protocol. It shows a communication throughput increase and also reduces the transmission delay experienced each data packet [4][5].

The exchange of control packets for CoopMAC is shown in Fig. 1. First, source node S senses the communication channel condition, busy or idle. If the channel is idle, source node S sends the RTS packet, reserving the channel for network allocation vector (NAV) duration. If not, source node S should wait the channel is idle and then send the RTS packet. When the relay node R receives the RTS packet and decodes it successfully, it responds with a helper ready-to-send (HTS) packet to the source S and the destination node D. After receiving the RTS packet followed by HTS packet, destination node D sends CTS packet to reserve the channel for cooperative communication via the relay node R. Even if destination node D does not receive the HTS from the relay node R, it sends the CTS packet to the source node S. But in this case, it reserves the channel for direct transmission between the source node S and the destination node D (Fig. 1(b)).

Once source node S receives the HTS packet from the relay node R and the CTS packet from the destination node D respectively, the cooperative transmission between source node S and destination node D via the relay node R starts (Fig. 1(a)). That is, source node S sends the data packet to relay node R and relay node R then forwards the packet received from source node S to destination node D. On the other hand, if source node S has not received the HTS packet from relay node R before the CTS packet is received from destination node D, it transmits the data packet directly to destination node D (Fig. 1(c)). After destination node D successfully receives the data packet from source node S, it sends an acknowledgment (ACK) packet to source node S. Otherwise, destination node D sends a negative acknowledgment (NACK), notifying source node S of the failure of transmission. In addition, if source node S receives no response from destination node D within a specific timeout period, it will also notice the failure of transmission to destination node D. For more complete details of CoopMAC protocol, please refers to [3][4].

III. Security Vulnerabilities in CoopMAC

Due to broadcast nature of the wireless channel and cooperative nature, cooperative communication suffers from various attacks.

For example, in Fig. 2, if source node S want to transmit data packet to destination node D using the relay node R, it first sends out the RTS, and the relay node R then reply with a HTS to source node S and destination node

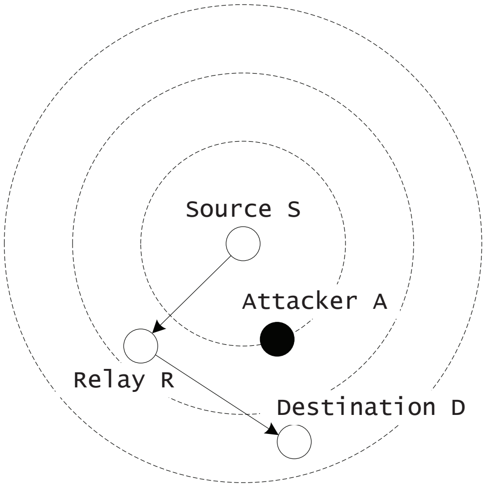


Figure 2. Example of DoS attack by neighboring node in CoopMAC

D. After receiving the RTS and the HTS, the destination node D finally sends a CTS to source node S. However, let's assume attacker node A is much closer to source node S than destination node D or it is between the source node S and the destination node D. In this case, attacker node A disguises itself as destination node D and responds with a CTS to source node S. There is no countermeasure to avoid this attack. That is, currently there is no suitable countermeasure mechanism to prevent a reply attack in the physical connection and authentication mechanism to authenticate destination node D. Therefore, an arbitrary attacker can respond with a CTS to neighboring nodes and thus it results in disruption of the normal cooperative transmission between nodes.

The goal of the attacker node is to obstruct the communication between source node and destination node. These attacker nodes would exploit the weakness in cooperation procedures, especially in the control packet exchange, and disguise themselves as legitimate relays. We will introduce some cases of attacks according to the control packet of CoopMAC next.

A. Attack on RTS Control Packet

In the CoopMAC as shown in Fig. 3(a), attacker node A sends the faked RTS to relay node R and destination node D, and then waits for the HTS from relay node R as well as CTS from destination node D. After the attacker node A receives the HTS and the CTS, it sends a fake data to the relay node R. Consequently, this attack results in a transmission disturbance in the RTS and the data packet from source node S. Accordingly, source node S can not start data transmission to relay node R.

On the other hand, as shown in Fig. 3(b), attacker node A intentionally sends the faked RTS to only destination node D. The legal RTS from source node S can be rejected by destination node D due to an illegal previous RTS received from attacker node A. Hence, CTS is sent from the destination node D to attacker node A, which causes source node S to continuously wait for the CTS from destination node D. As a result, normal cooperative communication between source node S and destination node D can not be guaranteed.

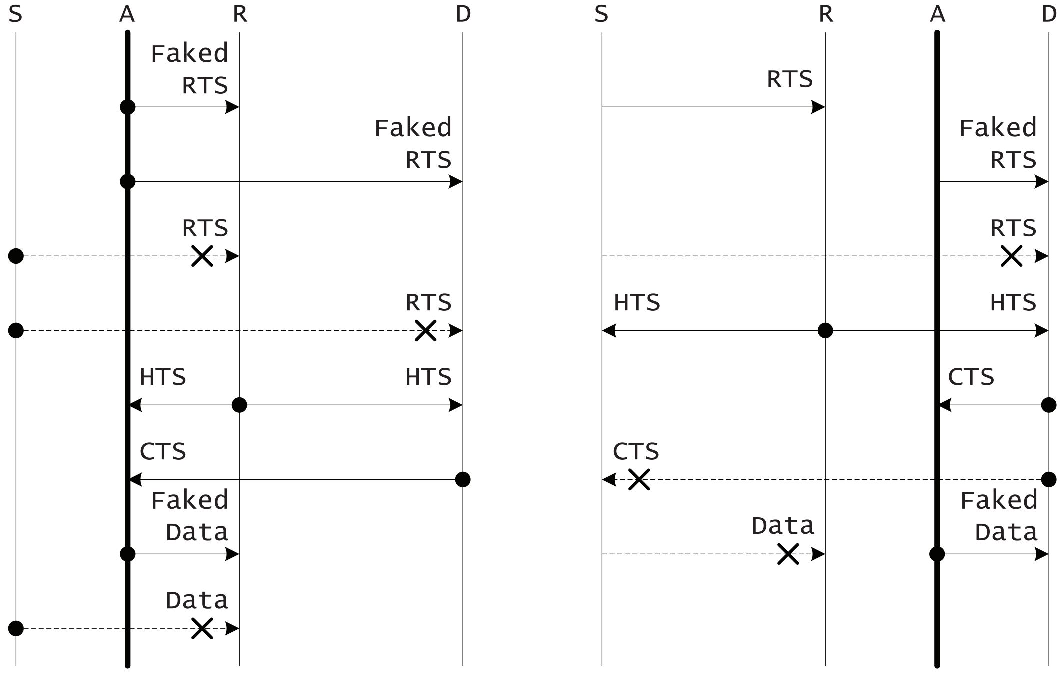
B. Attack on HTS Control Packet

As shown in Fig. 4(a), the faked HTS is sent from attacker node A to source node S and destination node D. Accordingly, the legal HTS from relay node R is denied by source node A and destination node D. Then, destination node D sends CTS to source node A. After receiving the faked HTS and CTS, source node S starts data transmission to attacker node A, but relay node R. Due to this false transmission to the attacker node A, cooperative communication between source node S and destination node D via relay node R is not established.

The potential security vulnerability from faked HTS in the CoopMAC is also shown in Fig. 4(b). In the case of sending faked HTS to only destination node D, since the destination node is typically not come to know of this, although the legal HTS is sent from the relay node R to destination node D, it is denied by destination node D. Then, the destination node D sends a CTS to source node S in order to notify that it successfully receives the control packet. This also means that attacker node A is an intended legitimate relay node forwarding data packet. Therefore, if relay node R receives the data packet from source node S, it doesn't forward data packet to the destination node D, but forwards it the attacker node A. Finally, the attacker node A denies cooperative communication service to the source node S by simply dropping the data packet it receives. It also spoofs an ACK, causing the source node S to wrongly conclude a successful transmission.

C. Attack on CTS Control Packet

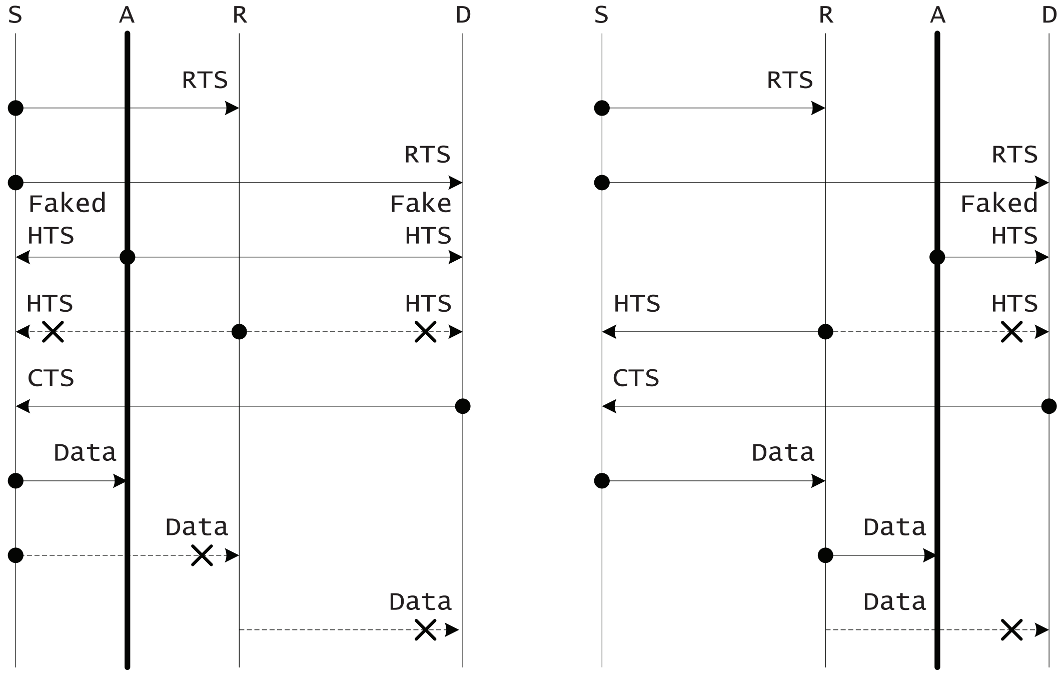
Fig. 5 shows a security vulnerability which caused by the faked CTS from attacker node A. In this case, the attacker node A sends a faked CTS to the source node S, informing the source node S that it is an intended recipient of future data packet. And, since the authentication is not applied to CTS packet, the legal CTS from destination D can be rejected by source node S due to a previous illegal CTS from attacker node A. Just after receiving the CTS from attacker node A, source node S transmits data packet to relay node R. Subsequently, the relay node R receives the data packet and then forwards received data packet to attacker node A. The attacker node A may try to deny communication service to the source by deliberately not forwarding data packet received from the relay node R. Consequently, cooperative communication between source node S and destination node D is not established.



(a) Faked RTS to R and D

(b) Faked RTS to D

Figure 3. Security vulnerability by RTS packet attack



(a) Faked HTS to S and D

(b) Faked HTS to D

Figure 4. Security vulnerability by HTS packet attack

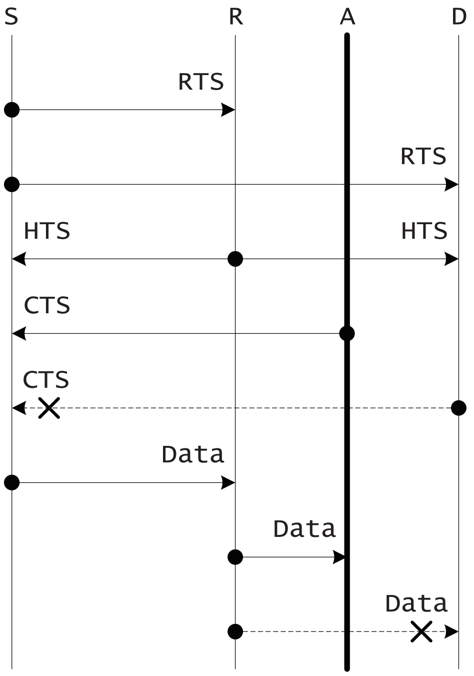


Figure 5. Security vulnerability by CTS packet attack

IV. Conclusion and Future Works

Security is a principal issue that must be resolved in order for the potential of cooperative communication networks to be fully exploited. However, security issues related to the design of cooperative network have largely not been considered.

CoopMAC is one such extension to the MAC sublayer. It was proposed to take advantage of cooperation, while remaining backward compatible with legacy IEEE 802.11. This paper presented the first case study of DoS attack in the CoopMAC. It also analyzed security vulnerabilities at each protocol stage while attacking a control packet exchanged among nodes. This work is the first comprehensive analysis of security vulnerability caused by DoS attack in CoopMAC. It can be significant in the use of designs of efficient authentication mechanism for secure CoopMAC. Moreover, our analytical results can be applied not only to cooperative network security, but also wireless sensor network (WSN) security design in general.

In the future, the authors will attempt to design and implement power-efficient authentication mechanism suitable for cooperative network. The plan is then to examine the effect that the proposed authentication mechanism has on the performance and efficiency of the cooperative transmission.

References

[1] A. Nosratinia, T. E. Hunter, and A. Hedayat, “Cooperative Communication in Wireless Networks,” *IEEE Communication Magazine*, Vol. 42, Issue. 10, pp. 74-80, 2004.

[2] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, “Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior,” *IEEE Trans. on Information Theory*, Vol. 50, No. 12, pp. 3062-3080, 2004.

[3] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *ANSI/IEEE Std 802.11*, 1999 Edition (R2003), 2003.

[4] P. Liu, Z. Tao, and S. Panwar, “A Cooperative MAC Protocol for Wireless Local Area Networks,” *IEEE ICC ’05*, pp. 2962-2968, 2005.

[5] T. Korakis. Z. Tao, S. Makda, and B. Gitelman, “It is Better to Give Than to Receive - Implications of Cooperation in a Real Environment,” *Springer LNCS 4479*, pp. 427-438, 2007.

[6] S. Makda, A. Choudhary, N. Raman, T. Korakis, Z. Tao, and S. Panwar, “Security Implications of Cooperative Communications in Wireless Networks,” *IEEE Sarnoff Symposium*, pp. 1-6, 2008.

[7] S. Kulkarni and P. Agrawal, “Safeguarding Cooperation in Synergy MAC,” *IEEE SSST ’10*, pp. 156-160, 2010.

[8] Y. Mao and M. Wu, “Tracing Malicious Relays in Cooperative Wireless Communications,” *IEEE Trans. on Information Forensics and Security*, Vol. 2, No. 2, pp. 198-207, 2007.

[9] Z. Han and Y. L. Sun, “Securing Cooperative Transmission in Wireless Communications,” *IEEE MobiQuitous ’07*, pp. 1-6, 2007.

[10] S. Dehnie, H. T. Sencar, and N. Memon, “Cooperative Diversity in the Presence of a Misbehaving Relay: Performance Analysis,” *IEEE Sarnoff Symposium*, pp. 1-7, 2007.

[11] S. Dehnie, H. T. Sencar, and N. Memon, “Detecting Malicious Behavior in Cooperative Diversity,” *IEEE CISS ’07*, pp. 895-899, 2007.

[12] S. Dehnie and N. Memon, “A Stochastic Model for Misbehaving Relays in Cooperative Diversity,”, *IEEE WCNS ’08*, pp. 482-487, 2008.

[13] H. Marques, J. Ribeiro, P. Marques, A. Zuquete, and J. Rodriguez, “A Security Framework for Cognitive Radio IP Based Cooperative Protocols,” *IEEE PIMRC ’09*, pp. 2838-2842, 2009.