Security Attack based on Control Packet Vulnerability in Cooperative Wireless Networks

Ki Hong Kim
The Attached Institute of ETRI
Daejeon, Korea
e-mail: hong0612@ensec.re.kr

***Abstract*—Cooperative wireless communication has been proposed as a way to improve channel capacity, robustness, reliability, delay, and coverage. Multiple research works have been done to support cooperative communication in the medium access control (MAC) layer. Synergy MAC is one of the MAC protocols that support cooperative communication using cooperative relay nodes. In this paper, some security attacks against control packets of Synergy MAC are identified and the potential security issues that arise in Synergy MAC due to these attacks are also discussed.**

Keywords–Synergy MAC; cooperative communication; control packet; security attack; security issue.

I. INTRODUCTION

Within the last ten years, cooperation communication in wireless networks has received significant attention. Cooperative wireless communication is an innovative communication scheme that takes advantage of the open broadcast nature of the wireless medium and the spatial diversity to achieve performance gain. It is also known to be essential for making ubiquitous communication connectivity a reality. In the cooperative wireless networks, when the source node transmits data 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. The destination node receives multiple data from the source node and the relay nodes and then combines them to achieve performance and quality improvement [1][2][3].

There are three major schemes employed by the relay node to forward data to the destination node: amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF). In AF scheme, relay node receives a noisy version of the transmitted original data and then amplifies and retransmits this noisy data to the destination node. On the other hand, in DF scheme, relay node decodes data transmitted by the source node and then retransmits the decoded data to the destination node. Finally, CF scheme works by forwarding incremental redundancy of original data by the relay node to the destination node [1][4].

Several protocols in the MAC layer have been proposed to utilize the concept of cooperative transmission. A typical example is Synergy MAC protocol [5][6]. Synergy MAC is an IEEE 802.11b [7] based cooperative MAC protocol for mobile ad hoc networks. Synergy MAC was proposed to take advantage of cooperation, while remaining backward compatible with legacy IEEE 802.11b. This protocol is able to alleviate the ill effects of signal fading by realizing spatial diversity and transmit data at rates higher than otherwise possible by allowing nodes with low signal-to-noise ratio (SNR) to destination utilize intermediate relay nodes. It also outperforms standard IEEE 802.11b and mitigate some of the fairness problems caused by multiple modulation schemes.

Security is a principal issue that must be resolved in order for the potential of cooperative wireless networks to be fully exploited. However, security issues related to the design of cooperative wireless networks have largely not been considered. In this paper, a comprehensive study of security attack based on control packet vulnerability in Synergy MAC is presented. Security issues at each handshaking procedure while attacking the control packets such as request-to-send (RTS) and clear-to-send (CTS) is analyzed and discussed. This work differs from previous works in that it concentrates on one significant aspect of a security issue in the Synergy MAC, namely security issue of Synergy MAC caused by attack against the control packets at handshaking mechanism.

The remainder of this paper is organized as follows. In Section II, I present some related works and security issues on cooperative wireless networks. In Section III, I give a brief description of the Synergy MAC protocol. In Section IV, I identify some possible security attacks against control packets of Synergy MAC and then discuss the security issues caused by these attacks. Finally, in Section V, I conclude the paper and present plans for future work.

II. RELATED WORKS

Due to the rapidly increasing popularity of cooperative wireless networks, there have been multiple research works regarding cooperative communication protocols and security issues for cooperative wireless networks. The work in [1] described cooperative wireless communication that enables single antenna mobiles to share their antennas. The [2] proposed and analyzed opportunistic relaying as a practical scheme that forms a cooperative diversity. The [3] introduced

 ISBN: 978-1-61208-256-1

an adaptive relay selection on demand with early retreat scheme to reduce the overall energy consumption significantly.

Some MAC protocols have been suggested to support cooperative transmissions in wireless networks. In [8], a new MAC protocol for the IEEE 802.11 [9], namely CoopMAC, was proposed and its performance was also analyzed. The Synergy MAC, an IEEE 802.11b [7] based cooperative MAC protocol for mobile ad hoc networks was studied in [5]. Also, COSMIC, a carrier sense multiple access/collision avoidance (CSMA/CA) based cooperative MAC protocol for wireless sensor network (WSN) with minimal control messages was proposed in [10], and cooperative MAC protocol of alleviating the problem from a pure MAC centric perspective, called CMAC was introduced to provide immediate improvements to the IEEE 802.11e [11] efficiency [4]. The [12] suggested a distributed MAC protocol, which uses an automatic relay selection with embedded relay collision avoidance and three-way handshaking to minimize signaling overhead.

Cooperative wireless communications are vulnerable to security attacks due to the open broadcast nature of the wireless communication channel and the cooperative transmissions with multiple transmitters. Several research groups have studied security issues including attacks, vulnerabilities, and mechanisms in cooperative wireless networks. The [13] formulated cooperative mechanisms for wireless networks with cooperative relays which help to give provable unconditional secrecy guarantees, while the [14] developed a framework for evaluating the trade-off between using cooperative transmissions or non-cooperative transmissions in sensor networks with a mix of malicious and non-malicious nodes. The [15] presented the distributed trust-assisted cooperative transmission mechanism handling relay's misbehavior as well as channel estimation error. The [16] described a security framework for leveraging the security in cognitive radio cooperative networks. The security vulnerabilities found in traffic adaptive cooperative wireless sensor-MAC (CWS-MAC), a flow specific medium access scheme were identified and analyzed in [17]. The work in [18] studied the coordinated denial of service (DoS) attacks against data packets using the concept of cooperative game theory on IEEE 802.22 [19] from the malicious nodes' perspective. The [20] proposed a detection technique of misbehaving nodes either based on the uniform most powerful (UMP) test or on the sequential probability ratio test (SPRT) in networks using CoopMAC and automatic repeat request (ARQ) protocols. The security concerns on data packets that a Synergy MAC introduces due to its reliance on a third party relay were discussed in [6]. Similarly, the potential security issues and vulnerabilities that arise in CoopMAC were addressed in [21][22].

In spite all the above mentioned researches, there is still no work that analyzes the security issues caused by the security attacks against control packets in the Synergy MAC.

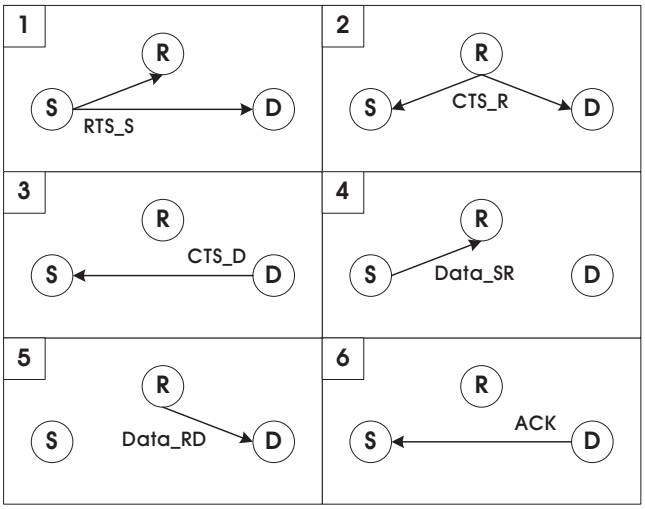

Figure 1. Handshaking mechanism followed by control packets exchange in Synergy MAC protocol.

Most of the previous works are focused on efficient and reliable cooperative transmission scheme using the relay node and identification of general security issues caused by the malicious relay node. In this paper, I discuss the potential security issues that arise in Synergy MAC due to security attacks against control packets. This work is the reasonable attempt to analyze and compare security issues from possible security attacks based on control packets vulnerabilities in Synergy MAC.

III. SYNERGY MAC

Synergy MAC is a MAC protocol based on the IEEE 802.11b's distributed coordination function (DCF) mechanism to realize cooperative transmission at the physical layer. It employs control packets like RTS and CTS for sensing the wireless medium to determine if it is free. The Synergy MAC is completely compatible with IEEE 802.11b and can be easily extended to suit other version of the legacy IEEE 802.11. It achieves higher rates of data transmission than IEEE 802.11b despite leveraging on the multi-rate capability of IEEE 802.11b.

The three-way handshaking procedure for Synergy MAC is depicted in Fig. 1. When a source node (S) wants to send data packets to destination node (D), it first senses the wireless channel condition, busy or idle. If the channel is idle, S sends the RTS packet (RTS_S) to the D, reserving the channel for network allocation vector (NAV) duration needed to transmit data packets. If not, S should wait the channel is idle and then send the RTS_S. When a relay node (R) overhears RTS_S transmission and decodes it successfully, it broadcasts a self addressed CTS packet (CTS_R). When the D receives a CTS_R from R soon after receiving a RTS_S from S, it sends CTS packet (CTS_D) to the S. This CTS_D is used to reserve the

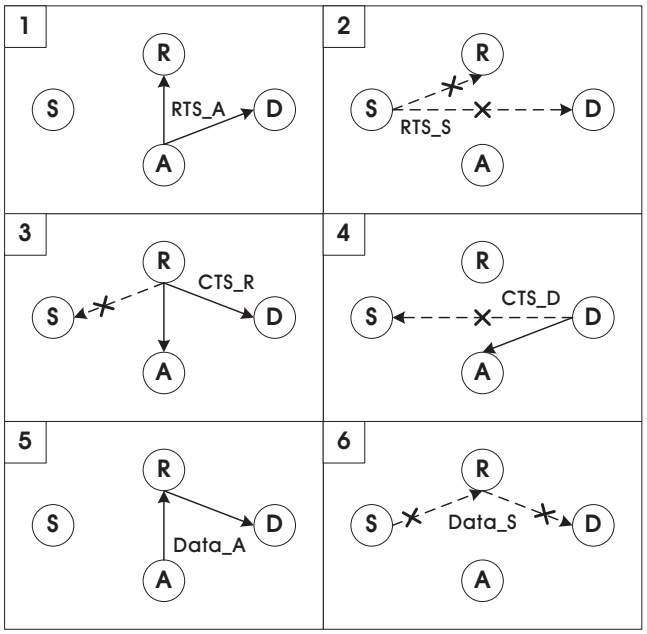

Figure 2. Source attack: false RTS transmission to relay and destination.

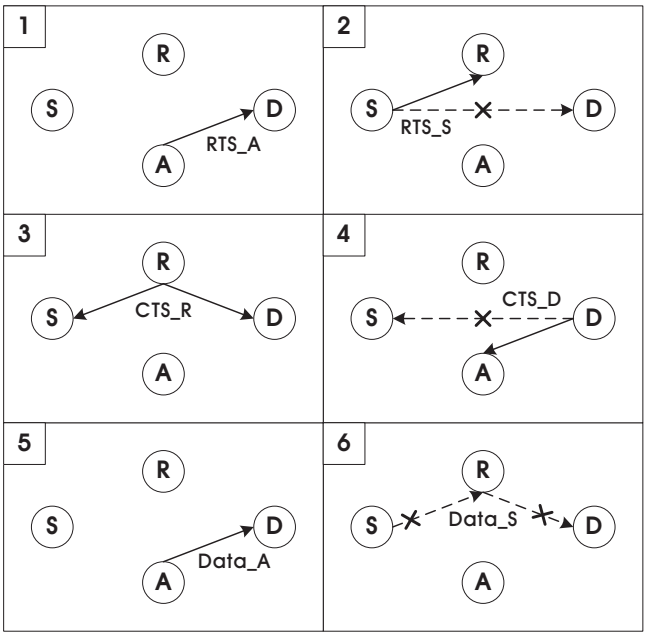

Figure 3. Source attack: false RTS transmission to destination.

channel for cooperative communication via the R. Once S receives the CTS_R from the R and the CTS_D from the D respectively, it starts transmitting its data packets ($Data\_SR$) to R. R then forwards the data packets ($Data\_SR = Data\_RD$) received from S to D. After D successfully receives $Data\_RD$ from R, it sends an acknowledgement packet (ACK) to S. Otherwise, D sends a negative acknowledgement packet ($NACK$), notifying S of the failure of cooperative transmission between S and D via the R. In addition, if S receives no response from D within a specific timeout period, it will also notice the failure of transmission to D. Data transmission cycle in Synergy MAC is complete when the S receives the ACK from the D. More details on Synergy MAC may be found in [5][6].

IV. Security Attack and Issue in Synergy MAC

Due to broadcast nature of the wireless transmission and cooperative transmission, Synergy MAC suffers from various attacks. For example, in Fig. 1, let's assume attacker node is closer to S than D or it is between the S and the D. In this environment, attacker node can disguise itself as D and respond with its CTS packet to S. There is no suitable countermeasure to prevent this attack and solution to authenticate D. Therefore, an attacker node close to the victim nodes can respond with a CTS packet to them thus it results in disruption of the normal cooperative transmission between nodes. The attackers' goal is focused on the network's performance, that means they want to disturb the communication between source node and destination node. They would exploit the weakness in cooperative procedure, especially in the control packets exchange, and disguise themselves as legitimate relay nodes to disturb the network's operation and to degrade the communication quality.

Security attacks based on the control packets resulting from attacker nodes can be classified into two categories: (1) false RTS attack and (2) false CTS attack. The former generates a false RTS packet in order to create the virtual jamming, while the latter generates a false CTS packet in order to disguise attacker as legitimate relay node or destination node. The followings introduce these attacks according to the control packets of Synergy MAC in greater detail.

A. Source Attack using False RTS

The first security attack is that of virtual jamming by an attacker node which deliberately sends false RTS packet to relay node and destination node. Let us take the case of Fig. 2. As shown in Fig. 2, attacker node (A) sends the false RTS packet (RTS_A) to relay node (R) and destination node (D). A then waits for the CTS packet (CTS_R) from R and CTS packet (CTS_D) from D. RTS_A causes R and D to deny legal RTS packet (RTS_S) from source node (S). This means that because R and D have already received the RTS packet from A, they reject the additional RTS packet from S. Once A receives the CTS_R and the CTS_D, it starts transmitting its false data packets ($Data\_A$) to the R. Thus, this attack blocks the transmission of the RTS_S and the data packets ($Data\_S$) from S. Consequently, S can not start its data packets transmission to R.

Next, A sends the RTS_A to only D. This scenario is depicted in Fig. 3. Since the authentication(or integrity) mechanism is not applied to the control packets exchange

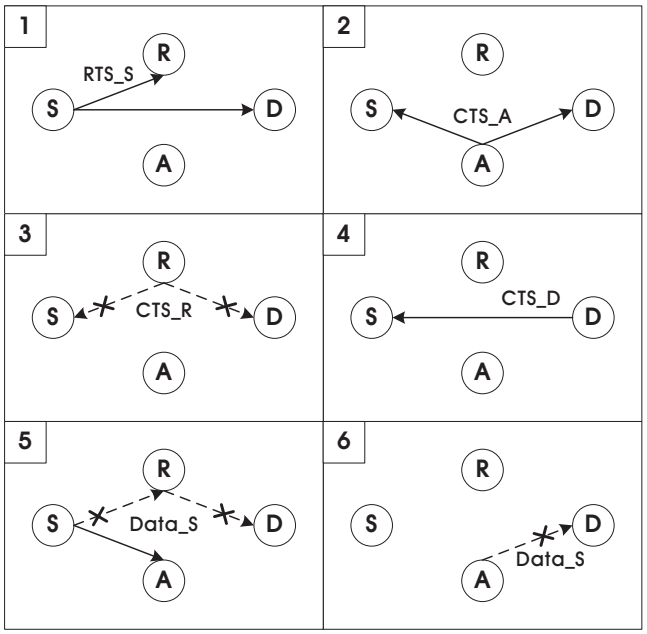

Figure 4. Relay attack: false CTS transmission to source and destination.

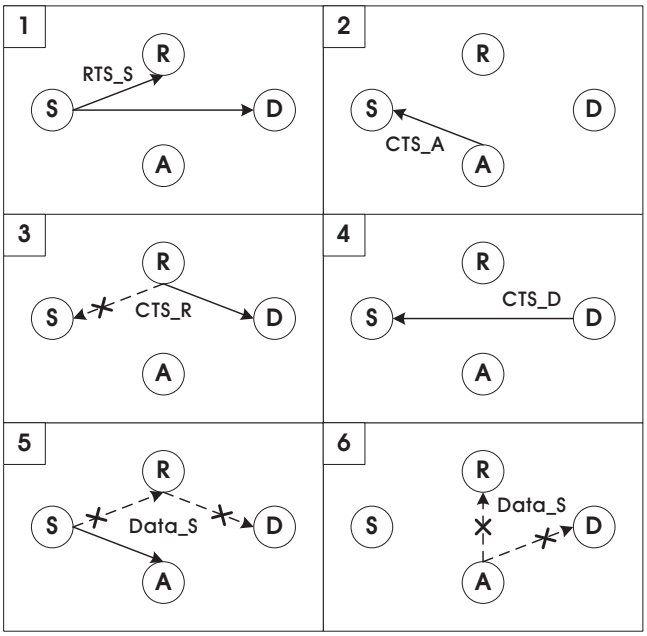

Figure 5. Relay attack: false CTS transmission to source.

between S and D, the legal RTS_S from S can be rejected by D due to an illegal previous RTS_A received from A. Accordingly, CTS_D is sent from the D to the A, not S. This means that the S continuously waits for the CTS_D from the D to finish the handshaking process. As a result, normal cooperative communication between S and D can not be guaranteed.

B. Relay Attack using False CTS

The second security attack is that of false CTS packet sending by the attacker node in order to disturb the relay node. An attacker node may try to deny relay node's legal CTS packet to source node and/or destination node by sending the false CTS packet, causing the source node and/or destination node to reject a legal CTS packet from relay node. As shown in Fig. 4, the false CTS packet (CTS_A) is sent from attacker node (A) to source node (S) and destination node (D). Accordingly, the legal CTS packet (CTS_R) from relay node (R) is denied by S and D. Then, D sends its CTS packet (CTS_D) to S. After receiving the CTS_A and CTS_D, S starts data packet ($Data\_S$) transmission to A, but R. A deliberately stops forwarding $Data\_S$ to R, which results in DoS attack caused by A. Due to this false transmission to A, cooperative communication between S and D via R is not established.

Fig. 5 illustrates another attack from attacker node's illegal CTS packet in the Synergy MAC. In the case of sending illegal CTS packet (CTS_A) to only source node (S), since the S is typically not come to know of this, although the legal CTS packet (CTS_R) is sent from relay node (R) to S, it is denied by S. Then, the destination node (D) sends a CTS packet (CTS_D) to S in order to notify that it successfully received the CTS_R. This also means that attacker node (A) is an intended legitimate relay node forwarding data packets ($Data\_S$). Therefore, S sends $Data\_S$ to A, not R. Finally, A denies cooperative communication to the S by simply dropping the $Data\_S$ it receives from S.

The potential relay node attack using illegal CTS packet is also shown in Fig. 6. Since the destination node (D) receives the illegal CTS packet (CTS_A) from attacker node (A), it rejects the legal CTS packet (CTS_R) from relay node (R). After receiving the CTS packet (CTS_D) from D, source node (S) sends its data packets ($Data\_S$) to R. If R receives the $Data\_S$ from S, it doesn't forward $Data\_S$ to D, but forwards it the A. A drops the $Data\_S$ received from R. It also spoofs an ACK, causing the S to wrongly conclude a successful cooperative transmission via R.

C. Destination Attack using False CTS

Fig. 7 shows a destination node attack which caused by the illegal CTS packet from attacker node. In this case, the attacker node (A) transmits a false CTS packet (CTS_A) to source node (S), informing the S that it is an intended recipient of future data packets ($Data\_S$). And, since the authentication(or integrity) mechanism is not applied to CTS_A, the legal CTS packet (CTS_D) from destination node (D) can be rejected by S due to a previous illegal CTS_A from A. Just after receiving the CTS_A from A, S transmits $Data\_S$ to relay node (R). Subsequently, the R receives the $Data\_S$ and then forwards it to A. The A may try to deny cooperative communication to S

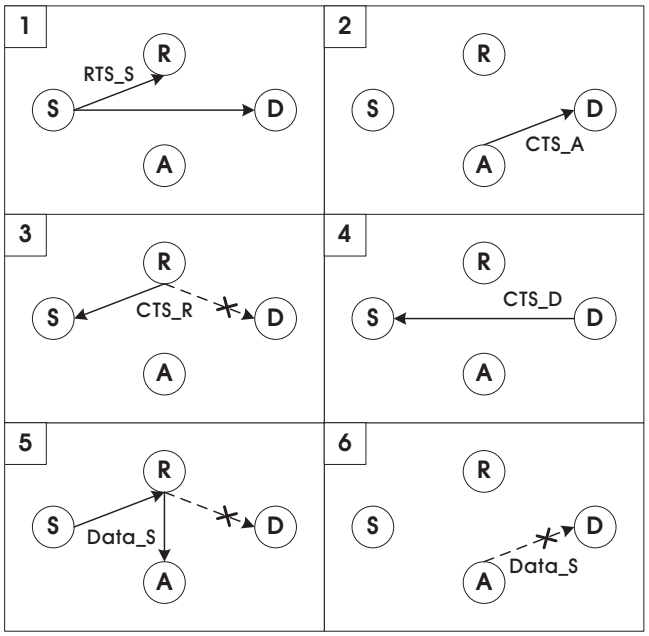

Figure 6. Relay attack: false CTS transmission to destination.

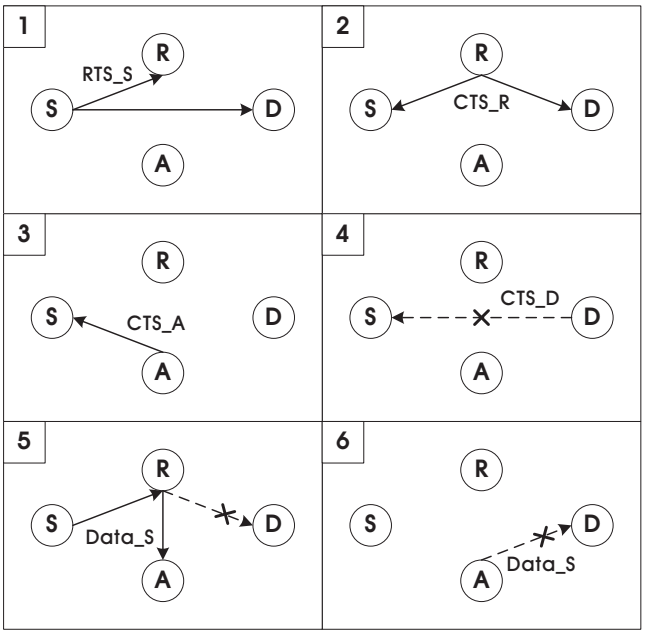

Figure 7. Destination attack: false CTS transmission to source.

by deliberately not forwarding $Data\_S$ received from R. Consequently, cooperative communication between S and D is not established.

V. Conclusion

This paper presented the case study of security attacks based on control packets (RTS and CTS) vulnerabilities in Synergy MAC. Furthermore, it analyzed security vulnerabilities at each handshaking stage while attacking control packets exchanged among nodes (source, destination, and relay). This study is the comprehensive analysis of security vulnerabilities caused by attacker node in Synergy MAC. It can be significant in the use of design of efficient authentication solutions for secure Synergy MAC. The analytical results can be extended to not only cooperative wireless network security, but also WSN security design in general.

As future work, the author plans to design and implement lightweight low-power authentication mechanism suitable for cooperative wireless networks. The plan is then to examine some effects with security cost, power consumption, and transmission performance using the proposed mechanism.

References

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

[2] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, “A Simple Cooperative Diversity Method Based on Network Path Selection,” IEEE Journal on Selected Areas in Communications, Vol. 24, pp. 659–672, 2006.

[3] H. Adam, C. Bettstetter, and S. M. Senouci, “Adaptive Relay Selection in Cooperative Wireless Networks,” IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1–5, 2008.

[4] S. Shankar, C. T. Chou, and M. Ghosh, “Cooperative Communication MAC (CMAC) – A New MAC Protocol for Next Generation Wireless LANs,” IEEE International Conference on Wireless Networks, Communications and Mobile Computing, pp. 1–6, 2005

[5] S. Kulkarni, P. S. Prasad, and P. Agrawal, “Enabling Cooperation in Mobile Ad Hoc Networks,” IEEE Sarnoff Symposium, pp. 1–5, 2009.

[6] S. Kulkarni and P. Agrawal, “Safeguarding Cooperation in Synergy MAC,” IEEE Southeastern Symposium on System Theory, pp. 156–160, 2010.

[7] IEEE Std. 802.11b–1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High Speed Physical Layer Extension in the 2.4GHz Band, 1999.

[8] P. Liu, Z. Tao, and S. Panwar, “A Cooperative MAC Protocol for Wireless Local Area Networks,” IEEE International Conference on Communications, pp. 2962–2968, 2005.

[9] IEEE Std. 802.11–1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[10] A. B. Nacef, S. M. Senouci, Y. Ghamri-Doudane, and A. L. Beylot, “COSMIC: A Cooperative MAC Protocol for WSN with Minimal Control Messages,” IFIP International Conference on New Technologies, Mobility and Security, pp. 1–5. 2011.

[11] IEEE 802.11e/D4.0, Draft Supplement to Part 11: Wireless Medim Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), 2002.

 ISBN: 978-1-61208-256-1

[12] C. T. Chou, J. Yang, and D. Wang, “Cooperative MAC Protocol with Automatic Relay Selection in Distributed Wireless Networks,” IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 526–531, 2007.

[13] E. Perron, S. Diggavi, and E. Telatar, “On Cooperative Wireless Network Secrecy,” IEEE Conference on Computer Communications, pp. 1935–1943, 2009.

[14] A. Aksu, P. Krishnamurthy, D. Tipper, and O. Ercetin, “On Security and Reliability Using Cooperative Transmission in Sensor Networks,” IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 1–10, 2010.

[15] Z. Han and Y. L. Sun, “Securing Cooperative Transmission in Wireless Communications,” IEEE International Conference on Mobile and Ubiquitous Systems: Networking & Services, pp. 1–6, 2007.

[16] H. Marques, J. Ribeiro, P. Marques, A. Zuquete, and J. Rodriguez, “A Security Framework for Cognitive Radio IP Based Cooperative Protocols,” IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications, pp. 2838–2842, 2009.

[17] T. O. Walker III, M. Tummala, and J. McEachen, “Security Vulnerabilities in Hybrid Flow-specific Traffic-adaptive Medium Access Control,” IEEE Hawaii International Conference on System Sciences, pp. 5649–5658, 2012.

[18] Y. Tan, S. Sengupta, and K. P. Subbalakshmi, “Analysis of Coordinated Denial-of-Service Attacks in IEEE 802.22 Networks,” IEEE Journal on Selected Areas in Communications, Vol. 29, pp. 890–902, 2011.

[19] IEEE P802.22/D0.1, Draft Standard for Wireless Regional Area Networks Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands, 2006.

[20] S. Dehnie and S. Tomasin, “Detection of Selfish Nodes in Networks Using CoopMAC Protocol with ARQ,” IEEE Transactions on Wireless Communications, Vol. 9, pp. 2328–2337, 2010.

[21] K. H. Kim, “Analysis of Security Vulnerability in Cooperative Communication Networks,” IARIA International Conference on Networking and Services, pp. 80–84, 2011.

[22] 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.

 ISBN: 978-1-61208-256-1