Security Issues in Cooperative MAC Protocols

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

***Abstract*—A lot of cooperative media access control (MAC) protocols have been proposed to support cooperative communications in wireless networks in the last few years. In this paper, the security vulnerabilities in some cooperative MAC protocols (e.g., COSMIC, VC-MAC, BTAC, and cooperative MAC for IEEE 802.11g) are analyzed. Channel-assisted authentication approach is also discussed to verify entities in cooperative MAC protocols. These analytical results should be significantly useful in the design of efficient authentication solutions for secure, cooperative MAC protocols.**

Keywords–Cooperative MAC protocols; vulnerability; authentication; physical layer security.

I. INTRODUCTION

A cooperative wireless network (CWN) is an emerging communication mechanism that takes advantages of spatial diversity among neighboring relay nodes, to achieve gains in performance and improved reliability. CWNs have attracted much attention within the last decade. In CWNs, when the source sends data to the destination, some nodes serve as relays by forwarding replicas of the source data to the destination. The destination receives multiple sets of data from the source and the relays, and then combines them. There are three major methods for forwarding from relay. First, for the amplify-and-forward (AF) method, after receiving a noisy version of the original data, the relay amplifies and retransmits noisy data to the destination. Second, for the decode-and-forward (DF) method, the relay decodes data from the source and then retransmits the decoded data to the destination. Finally, in the compress-and-forward (CF) method, the relay forwards incremental redundancy of the original data to the destination. The destination receives multiple data sets from the source and multiple relays; then it combines them to achieve gains in performance and quality [1][2].

Due to the rapid growth and evolution of CWNs, much research has been done to propose a cooperative MAC protocol that supports cooperative communication in wireless networks such as wireless sensor networks (WSNs) and vehicular networks. In other work, a new carrier-sense, multiple-access, collision-avoidance (CSMA/CA)-based MAC protocol, called the cooperative MAC protocol for WSN with minimal control message (COSMIC), was proposed to support cooperative relaying with minimum overhead [3]. The vehicular cooperative MAC (VC-MAC) was designed for gateway downloading in vehicular networks [4]. It leverages the advantages of both cooperative communication and spatial re-usability, maximizing system throughput. A busy-tone-based cooperative MAC protocol (BTAC) for wireless local area networks (WLANs) has also been proposed [5]. An efficient cooperative MAC protocol based on IEEE 802.11g was proposed [6], which can be extended to 802.11n. Easy comparison has been made possible by an analytical model of the power consumption of the various MAC protocols [7].

CWNs are vulnerable to security attacks due to the open broadcast nature of the wireless channel and the use of cooperative transmission involving multiple transmitters. There have been a number of studies regarding security issues, including attacks and vulnerabilities, in the cooperative MAC protocols. One study introduced the case study of security attacks based on control-packet vulnerabilities in Synergy MAC [8], while another addressed the potential security issues and vulnerabilities that arise in CoopMAC [9]. The security vulnerabilities found in traffic adaptive-cooperative, wireless sensor-MAC (CWS-MAC) have been identified and analyzed [10]. Coordinated denial-of-service (DoS) attacks against data packets on IEEE 802.22 have been studied from the perspective of malicious nodes [11]. A detection scheme to mitigate malicious relay behavior in a cooperative environment has been proposed [12][13][14]. Similarly, the selfish-behavior attack/detection model and the attack strategies of smart selfish nodes have been analyzed [15]. A secure, cooperative-data-downloading framework for paid services in vehicular ad hoc networks (VANETs) has also been proposed [16].

In spite of all the work mentioned above, security vulnerabilities in many cooperative MAC protocols have not yet been analyzed (i.e., COSMIC, VC-MAC, BTAC, and cooperative MAC for IEEE 802.11g). In this paper, some security attacks against COSMIC, VC-MAC, BTAC, and cooperative MAC for IEEE 802.11g are disclosed, and security vulnerabilities that arise in them due to attacks, are then analyzed. The emerging, channel-assisted authentication mechanism using physical layer characteristics is also discussed to verify entities in cooperative MAC protocols. To my knowledge, this is the first comprehensive case study of security issues caused by possible security attacks on COSMIC, VC-MAC, BTAC, and cooperative MAC for IEEE

 ISBN: 978-1-61208-330-8

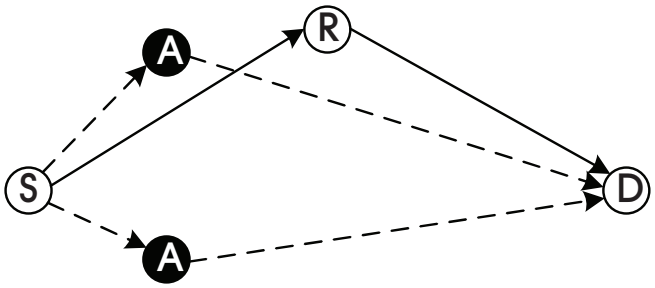

Figure 1. Example of Security Attack in Cooperative Wireless Networks.

802.11g.

The remainder of this paper is organized as follows. In Section II, a brief description of some cooperative MAC protocols is provided. In Section III, some possible security attacks are disclosed and then the security vulnerabilities caused by these attacks are analyzed. In Section IV, channel-assisted authentication mechanism is discussed to authenticate entities in cooperative MAC protocols. Finally, in Section V, conclusions are presented along with plans for future work.

II. Cooperative MAC Protocols

Cooperative wireless communication is an innovative communication scheme that takes advantage of the open broadcast nature of the wireless medium, and its spatial diversity, to improve channel capacity, reliability, robustness, delay, and coverage. It is known to be essential for making ubiquitous communication connectivity a reality. Multiple protocols in the MAC layer have been suggested to utilize the concept of cooperative transmission.

COSMIC is a cooperative MAC protocol for WSN with minimal control packets. It uses only one control packet, request-for-relay (RFR), for relay selection. In COSMIC, the relay selection is decided using both the channel-state information (CSI) and the remaining energy. COSMIC is able to increase network lifetime by about 25% and the delivery ratio by 5 times [3].

VC-MAC is a cooperative MAC protocol for vehicular networks. It is composed of four stages, namely, the gateway broadcast period, information exchange period, relay set selection period, and data forwarding period. VC-MAC exploits the concept of cooperative communication and takes advantages of the broadcast nature of the wireless medium to maximize throughput. This protocol also leverages spatial diversity and user diversity to overcome the unreliability under many broadcast scenarios. VC-MAC significantly increases system throughput compared with existing strategies [4].

BTAC is a cooperative MAC that increases throughput in multi-rate WLANs. A busy tone signal of only one-time-slot length is used to improve the throughput performance and reduce relay. It is known to improve throughput performance by at least 35% and reduce system delay, compared to the

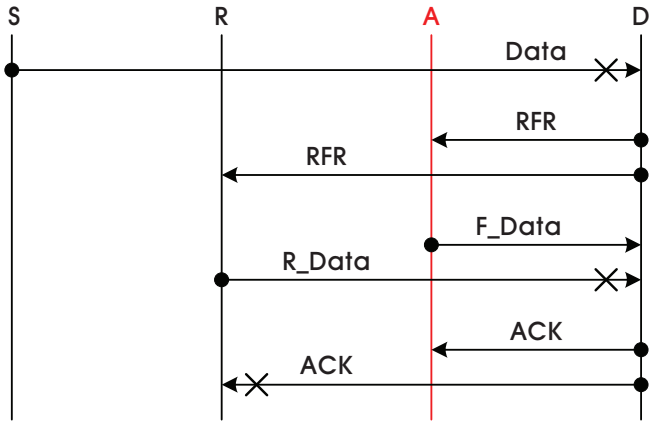

Figure 2. Security Vulnerability in COSMIC.

IEEE 802.11b MAC protocol. BTAC is compatible with IEEE WLAN [5].

To increase performance and reduce energy consumption in previous versions of cooperative MAC for IEEE 802.11b, a new cooperative MAC protocol for IEEE 802.11g (being extended to 802.11n) was proposed. It can support ten different transmission rates (1, 2, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps) and can efficiently reduce the time for selecting better relays, by partitioning the relays with similar transmission rates, into the same groups [6].

III. Security Vulnerability in Cooperative MAC Protocols

Cooperative MAC protocols suffer from vulnerability to various security attacks due to the open broadcast nature of the wireless channel and the use of cooperative communication with multiple relays [8][9].

For example, in Fig. 1, let us assume that the attacker is closer to source than to the relay, or that it is between source and relay. In this environment, attacker can disguise itself as relay to allow its illegal packet to get to source and destination. There is no suitable countermeasure to prevent this attack, nor any way to authenticate legitimate relay. Therefore, the result is disruption of the normal cooperative transmission between source and destination.

Attackers are focused on network performance, which means they want to disturb the communication between source and destination. They would exploit the weakness in the cooperative procedure, especially in the control packet exchange, and disguise themselves as legitimate relays to disturb the network operation, and to degrade the wireless channel quality. Security attacks based on control packets can be classified into two categories: faked request-to-send (RTS) attacks and faked clear-to-send (CTS) attacks. The former generates a false RTS packet in order to achieve virtual jamming of source, while the latter generates a false

 ISBN: 978-1-61208-330-8

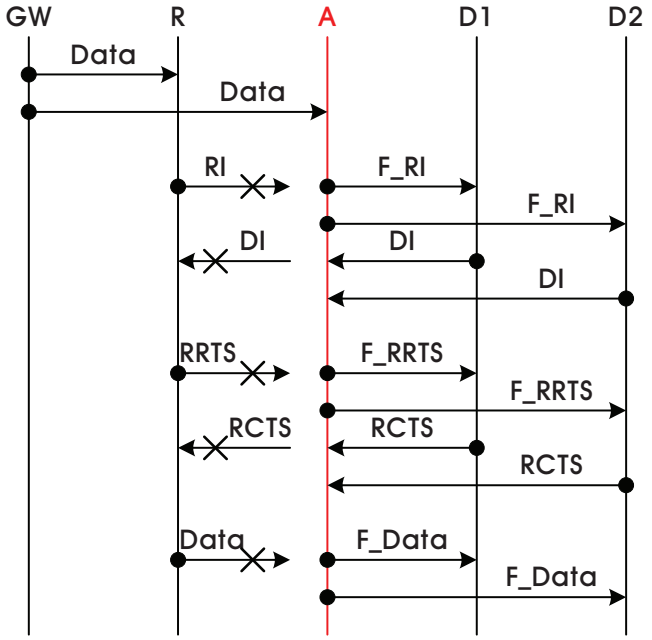

Figure 3. Security Vulnerability in VC-MAC.

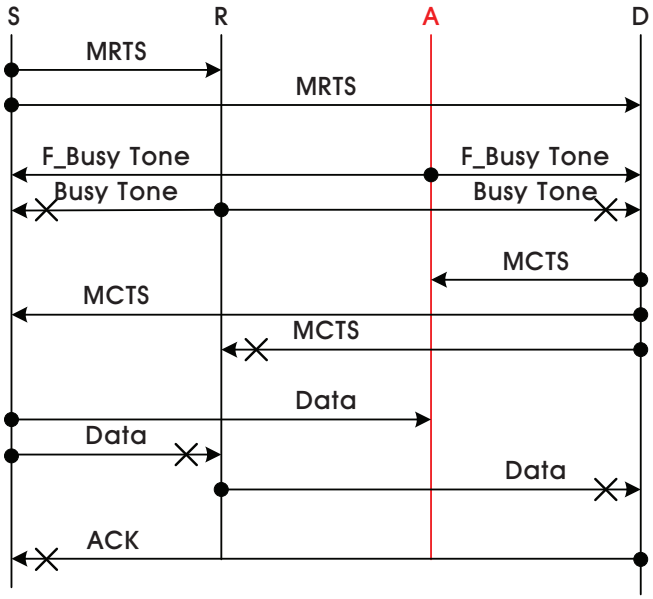

Figure 4. Security Vulnerability in BTAC.

CTS packet in order to disguise attacker as legitimate relay or destination.

A. Security Vulnerability in COSMIC

Fig. 2 shows a destination attack caused by faked data (F_Data) from attacker. In this case, attacker deliberately transmits its F_Data to destination, informing it that attacker is a legitimate relay.

As shown in Fig. 2, in COSMIC, source sends data to destination, which receives the data. Neighbors, relay and attacker overhear it. If destination is able to decode the data, it sends an acknowledgment (ACK) to source. In this case, no relaying is needed. However, if destination is not able to decode the data, a cooperative relaying is engaged.

When destination doesn't successfully receive data from source, it sends a request-for-reply (RFR) to relay to express its need for a relaying. Destination then waits for the data (R_Data) from relay. The R_Data is the relayed copy of the data. Since attacker is close to relay, it is able to receive the RFR. After receiving the RFR from destination, attacker sends its faked data (F_Data) to destination. Finally, destination sends an ACK to attacker to notify that it successfully received the data. This blocks the transmission of R_Data from relay. Consequently, cooperative communication between source and destination is not established.

B. Security Vulnerability in VC-MAC

Fig. 3 illustrates a security attack using faked relay information (F_RI) from an attacker in the VC-MAC.

In the VC-MAC, after the gateway, which is deployed along the roadside, senses the channel is idle, it sends data directly with no handshaking procedure. After the broadcast of the gateway, relay and attacker, which both received the data, become potential relays. Attacker sends faked relay information (F_RI) to two destinations (Destinations 1 and 2) before the transmission of relay information (RI) from relay. Attacker then waits for destination information (DI) from destinations 1 and 2. Since the authentication (or integrity) mechanism is not applied to the control packets exchanged between relay, and destinations 1 and 2, the legal RI from relay may be rejected by destinations 1 and 2 due to illegal previous F_RI received from attacker. This means that because destinations 1 and 2 have already received RI from attacker, they reject additional RI from relay. Once attacker receives two sets of DI, it transmits a faked relay request-to-send (F_RRTS). After receiving the relay clear-to-send (RCTS), attacker makes a faked data (F_Data) transmission to destinations 1 and 2. As a result, normal cooperation between relay and destination 1 or 2 cannot be guaranteed.

C. Security Vulnerability in BTAC

The potential security attack in BTAC is also shown in Fig. 4. An attacker sends a faked busy tone (F_BusyTone) to inform the source and destination that it is an intended helper to forward the data received from source.

Source sends modified RTS (MRTS) to relay and destination. Attacker near relay or destination comes to know of this. The F_BusyTone is sent from attacker to source and destination. This means that attacker is an intended legitimate relay for forwarding data. Accordingly, since the authentication (or integrity) mechanism is not applied to F_BusyTone, the legal busy tone (BusyTone) from relay is denied by source and destination due to the previous illegal

 ISBN: 978-1-61208-330-8

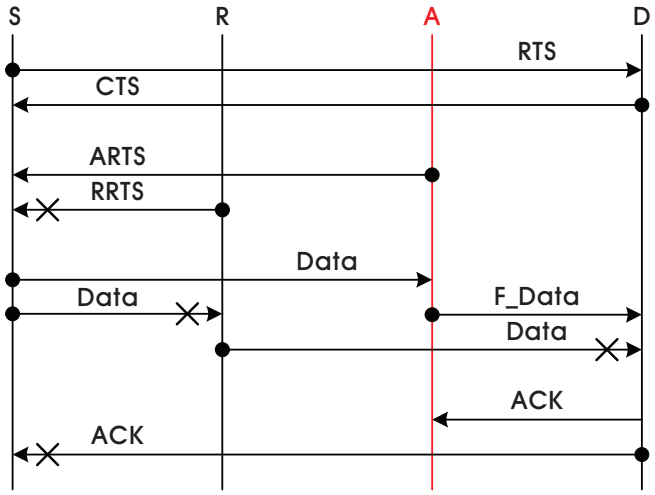

Figure 5. Security Vulnerability in Cooperative MAC for IEEE 802.11g or 802.11n.

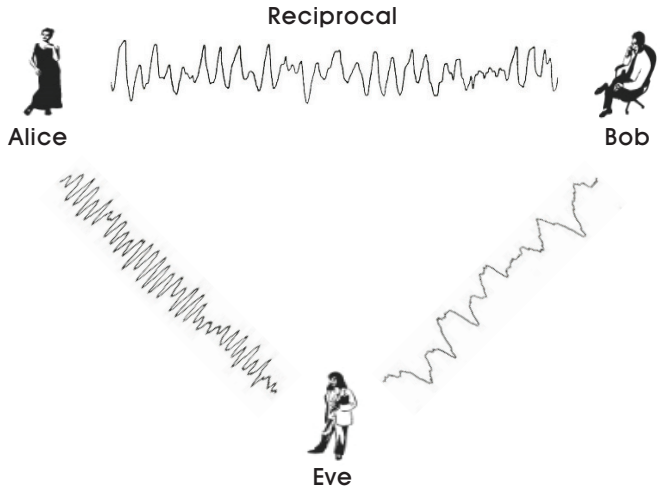

Figure 6. Example of Security Community with Alice (Legitimate), Bob (Legitimate), and Eve (Illegitimate).

F_BusyTone received from attacker. Then, destination sends its modified CTS (MCTS) to attacker and source. Source sends data to attacker, not to relay. Finally, attacker denies cooperative communication service to source by simply dropping the data it receives from source, or forwarding faked data to destination. Due to this false data transmission from source to attacker, cooperative communication between source and destination via relay is not established.

D. Security Vulnerability in Cooperative MAC for IEEE 802.11g or 802.11n

Fig. 5 shows a security vulnerability caused by the illegal RTS packet (ARTS) from attacker in cooperative MAC for IEEE 802.11g.

When source finds a free channel and it can send data to destination, it will send an RTS to destination and wait for CTS from destination. Since attacker, as well as relay, can overhear both RTS and CTS, attacker can communicate with both source and destination so that it can serve as a legitimate helper candidate between source and destination. Just after overhearing both RTS and CTS, attacker calculates the data rates from itself to source and destination. Attacker then replies ARTS to tell source that it can help with transmission. This means that attacker is an intended legitimate relay forwarding data. Since source receives illegal RTS (ARTS) from attacker, it rejects the legal RTS (RRTS) from relay. Then, source sends data to attacker, not relay. If attacker receives data from source, it simply drops the data received or forwards faked data (F_Data) to destination. It may also spoof an acknowledgment (ACK), causing destination to wrongly conclude a successful cooperative transmission via relay.

IV. Channel-Assisted Authentication Mechanism

In order to prevent the security attacks inherent in cooperative MAC protocols and verify entities more efficiently, a channel-assisted authentication mechanism using physical layer properties of wireless channel is discussed. The following four main characteristics of wireless channel can allow the wireless channel to be used as a means to authenticate the legitimate entity [17][18].

- The impulse response for time-variant wireless channel decorrelates quite rapidly in space.
- Wireless channel also changes in time, which results in a natural refresh for a channel-assisted security mechanism.
- The wireless channel is reciprocal in space.
- The time variation is slow enough so that the channel response can be accurately estimated within the channel coherent time.

In the typical environment shown in Fig. 6, three entities (Alice, Bob, and Eve) are potentially located in spatially separated positions. Alice and Bob are the two legitimate entities, and Eve is the illegitimate entity. Alice is the transmitter that initiates communication and sends data, while Bob is the intended receiver. Eve is an attacker that injects false signals into the channel in the hope of spoofing Alice. The main security goal is to provide authentication service between Alice and Bob. The legitimate receiver (Bob) should have to distinguish between legitimate signals from legitimate transmitter (Alice) and illegitimate signals from attacker (Eve).

As depicted in Fig. 6, let us suppose that Alice transmits data to Bob at a sufficient rate to ensure temporal coherence between successive data sets. In addition, while trying to impersonate Alice, Eve wishes to convince Bob that she is

 ISBN: 978-1-61208-330-8

Alice. To provide authentication between Alice and Bob, Bob first uses the received signal from Alice to estimate the channel response. He then compares this signal with a previous signal version of the Alice-Bob channel. If the two channel responses are close to each other, Bob concludes that the source of the data is the same as that of the previously transmitted data. Otherwise, Bob concludes that the transmitter is not Alice [18][19]. Using this uniqueness of the Alice-Bob wireless channel, it is possible to distinguish between legitimate transmitter (Alice) and illegitimate one (Eve). It is caused by the fact that the wireless channel decorrelates in space, so the Alice-Bob channel is totally uncorrelated with the Alice-Eve and Bob-Eve channels if Eve is more than an order of a wavelength away from Alice and Bob.

V. CONCLUSIONS

Security is the principal issue that must be resolved in order for the potential of CWNs to be fully exploited. This work provides a comprehensive analysis of the security issues caused by attackers for cooperative MAC protocols such as COSMIC, VC-MAC, BTAC, and cooperative MAC for IEEE 802.11g. Security vulnerabilities are analyzed at each handshaking stage, while attacking control packets are being exchanged among nodes (source, destination, and relay). It also discusses that a channel-assisted authentication mechanism is applicable to enhance and supplement conventional cryptographic authentication mechanism for cooperative MAC protocols. These results should be significantly useful in the design of efficient authentication mechanisms for secure, cooperative MAC protocols.

In the future, the author plans to design and implement a lightweight, low-power authentication (or integrity) mechanism using physical layer properties suitable for CWNs. The plan is then to examine the effects of the proposed mechanism on security cost, power consumption, and transmission performance.

REFERENCES

[1] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative Communication in Wireless Networks," IEEE Communication Magazine, vol. 42, October 2004, pp. 74-80.

[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, March 2006, pp. 659-672.

[3] A. B. Nacef, S.-M. Senouci, G.-D. Yacine, and A.-L. Beylot, "COSMIC: A Cooperative MAC Protocol for WSN with Minimal Control Messages," IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011), February 2011, pp. 1-5.

[4] J. Zhang, Q. Zhang, and W. Jia, "VC-MAC: A Cooperative MAC Protocol in Vehicular Networks," IEEE Trans. on Vehicular Technologies, vol. 58, March 2009, pp. 1561-1571.

[5] S. Sayed and Y. Yang, "BTAC: A Busy Tone Based Cooperative MAC Protocol for Wireless Local Area Networks," International Conference on Communication and Networking in China (ChinaCom 2008), August 2008, pp. 403-409.

[6] J.-P. Sheu, J.-T. Chang, C. Ma, and C.-P. Leong, "A Cooperative MAC Protocol Based on 802.11 in Wireless Ad hoc Networks," IEEE Wireless Communications and Networking Conference (WCNC 2013), April 2013, pp. 416-421.

[7] J. Rousselot, A. El-Hoiydi, and J.-D. Decotignie, "Low Power Medium Access Control Protocols for Wireless Sensor Networks," European Wireless Conference (EW 2008), June 2008, pp. 1-5.

[8] K. H. Kim, "Security Attack based on Control Packet Vulnerability in Cooperative Wireless Networks," IARIA International Conference on Networking and Services (ICNS 2013), March 2013, pp. 123-128.

[9] K. H. Kim, "Analysis of Security Vulnerability in Cooperative Communication Networks," IARIA International Conference on Networking and Services (ICNS 2011), April 2011, pp. 80-84.

[10] T. O. Walker III, M. Tummala, and J. McEachen, "Security Vulnerabilities in Hybrid Flow-specific Traffic-adaptive Medium Access Control," Hawaii International Conference on System Sciences (HICSS 2012), January 2012, pp. 5649-5658.

[11] 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, April 2011, pp. 890-902.

[12] Y. Mao and M. Wu, "Tracing Malicious Relays in Cooperative Wireless Communications," IEEE Trans. on Information Forensics and Security, vol. 2, June 2007, pp. 198-207.

[13] S. Dehnie, H. T. Sencar, and N. Memon, "Detecting Malicious Behavior in Cooperative Diversity," Conference on Information Sciences and Systems (CISS 2007), March 2007, pp. 895-899.

[14] S. Dehnie and S. Tomasin, "Detection of Selfish Nodes in Networks Using CoopMAC Protocol with ARQ," IEEE Trans. on Wireless Communications, vol. 9, July 2010, pp. 2328-2337.

[15] H. Li, M. Xu, and Y. Li, "The Research of Frame and Key Technologies for Intrusion Detection System in IEEE 802-11-based Wireless Mesh Networks," International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2008), March 2008, pp. 455-460.

[16] Y. Hao, J. Tang, and Y. Cheng, "Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks," IEEE Journal on Selected Areas in Communications/Supplement, vol. 31, September 2013, pp. 523-537.

[17] S. Mathur, A. Reznik, Y. Chunxuan, and R. Mukherjee, "Exploiting the Physical Layer for Enhanced Security," IEEE Wireless Communications, vol. 17, October 2010, pp. 63-70.

[18] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," IEEE Trans. on Wireless Communications, vol. 7, July 2008, pp. 2571-2579.

[19] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," IEEE Wireless Communications, vol. 17, October 2010, pp. 56-62.

 ISBN: 978-1-61208-330-8