http://dx.doi.org/10.14400/JDC.2014.12.12.323

Security Characteristics of D-MAC in Convergence Network Environment

Jinkeun Hong
Div. of Information and Communication, Baekseok University

융합망 환경에서 D-MAC의 보안 특성

홍진근
백석대학교 정보통신학부

Abstract D-MAC protocol is used convergence network, which is designed to connect wireless link between things. This protocol is supported to local data exchange and aggregation among neighbor nodes, and distributed control packet from sink to sensor node. In this paper, we analysis about efficiency of power consumption according to whether or not security authentication of D-MAC in convergence network. If authentication scheme is applied to MAC communication, it is related to power consumption of preamble whether or not with and without authentication process. It is reduced to energy consumption against denial attack of service, when it is applied to authentication. Future work will take the effort to deal with security authentication scheme.

Key Words : MAC, DoS, Security, Communication, Sensor, Power, Convergence

요 약 융합망에 사용되는 D-MAC 프로토콜은 사물간 무선링크를 연결하기 위해 설계된 프로토콜이다. 이 프로토콜은 이웃 노드 가운데 로컬 데이터 교환과 수집을 위해 제공되고, 싱크로부터 센서 노드로 제어패킷과 관심 패킷이 분배된다. 본 논문에서는 융합망의 D-MAC 보안 인증 적용 여부에 따른 전력소모 효율성에 대해 분석하였다. 인증기법이 MAC 통신에 적용될 경우, 인증처리 유무에 따라 프리앰블의 에너지 소비 여부가 연관이 된다. 인증이 적용될 경우 서비스 공격에 대응하여 에너지 소비가 감소된다. 향후 보안 인증기법에 관련한 연구를 수행할 계획이다.

주제어 : MAC, 서비스거부공격, 보안, 통신, 센서, 전력, 융합

1. Introduction

In general, the MAC protocol in wireless convergence sensor communication is used to deside the access time during which is contending between nodes among wireless communication medium. The quality of service (QoS) issue of sensor network is related to throughput, latency, loss ration, delivery ratio, energy consumption, reliability. Wireless convergence sensor network(WSN) is network of

* 본 논문은 2014년 백석대학교 산학협력단의 학술연구비에 의하여 지원되었음
Received 21 October 2014, Revised 24 November 2014
Accepted 20 December 2014
Corresponding Author: Jin-Keun Hong(Baekseok University)
Email: jkhong@bu.ac.kr

ISSN: 1738-1916

sensors for communication on wireless link. These convergence sensors may be installed in an unattendedenvironment with limited computation and sensing capabilities.

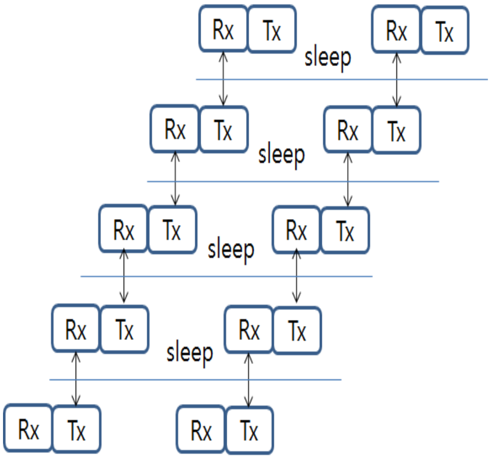
However issue of MAC protocol is to design energy efficient protocol. Many MAC protocol is consumed due to collision, overhearing, idle listening. Therefore it is important to design and analysis suitable MAC protocol which reduce energy consumption. In the related research, Eoin et. al reviews issue of energy and reliability optimal MAC for wireless convergence sensor network.

This paper demonstrates low power and reliable communication problem in each MAC protocol such as X-MAC, A-MAC, S-MAC, BoX-MAC, Wise MAC[1]. Mahendra and Sushil presented mathematical energy model to evaluate the energy consumption, based on current traffic conditions such as switching energy, sleeping energy, listening energy, overall energy, receiving energy and transmission energy[2]. Saylee S. Thorat and S. D. Markande proposed reinvented fuzzy logic secure media access control protocol to improve life span of wireless sensor networks[3]. This scheme is solution against DoS atack such as collision attack, unfairness attack, exhaustion attack. Cristina Cano et. al proposed addressing limitation problem by the improvement of receiver initiated MAC protocols with scheduling for WSNs by applying scheduling[4]. Mouzehkesh et. al analysis about the traffic diversity problem in WBAN and propose fuzzy scheme of mac protocol[5]. Messaoud et. al present duo MAC, which is an asynchronous cascading wake up scheduled MAC protocols for heterogenous traffic forwarding in low power network[6]. Attiah et. al present EE-MAC, which is achieved a low duty cycle and low energy consumption through optimized sleep intervals[7]. Wei et. al propose priority MAC, which is medium access control control protocol for critical in WSN. It is provided theoretical analysis of average access delay for different traffic priorities in [8]. Xiuming et. al report about real time communication protocol for wireless body area networks in [9]. This paper is analyzed slot timing of warming up, transmission, receiving state in IEEE802.15.4 radio timing profiles. The Tx slot time is scheduled from slot start, TX state, ACK waiting, to slot end. On the contrary, the Rx slot include slot start, Rx state, ACK sending, slot ending. In Rx state, if there is received packet header, then it is prepared ACK. Vivek et. al is compared performance of different MAC protocols such as CSMA, TDMA, Federated MAC in [10]. The QoS issue of sensor network is related to throughput, latency, loss ration, delivery ratio, energy consumption, reliability. Especially, it is significant to analysis energy consumption in wireless convergence sensor network environment. However no matter how a good communication protocol is designed and consumed power energy, if communication protocol does not be considered security vulnerability issue, there is limited in terms of performance of communication service. It is critical to consider denial issue of service and check MAC communication effect in wireless sersor network. Therefore in this respect, this paper review energy performance of D-MAC protocol out of convergence sensor MAC protocol services. It is considered power efficiency on transmission path in case of service denial attack.

This is believed to be the analysis of security vulnerability and its power consumption caused by service denial attack of parent node's active state in D-MAC protocol. The analytical results can be used to design a power efficient communication scheme in wireless convergence sensor MAC communication security. The remaining paper is organized as follows. In section 2, we describe D-MAC convergence communication protocol environment. Next, in section 3, we analyze the security vulnerabilities of D-MAC protocol and compare the power consumption at each stage of D-MAC protocol procedure according to denial of service attack. Finally in section 4, we review our conclusions.

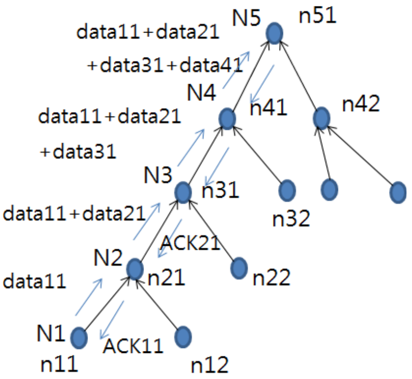
2. D-MAC convergence communication protocol

D-MAC is protocol which has three pattern in wireless convergence sensor network application. First it is exchanged and aggregated local data among nearby nodes. Second it send control packet from the sink node to sensor node. Third it gathered data from sensor node to sink node. The communication schedule of D-MAC protocol is shown as follows in Fig.1. D-MAC is good latency unlike CTS/RTS period scheme. But the collision avoidance scheme is depend upon network access rate according to network condition. In case of D-MAC, it has three interval such as receiving, sending, sleep period. In the receiving state, it is expected to data packet and send ACK packet to the sender. D-MAC has different duty cycle according to level of node tree. If it is equal to depth level, it is equal to duty cycle.



[Fig. 1] Wakeup Schedule

In the sending state, it is tried to send packet from node to next hop and receive ACK packet. In the sleep state, it is tuned off to down of power consumption. On multiple hops, it is increased duty cycle due to node and if there are multiple packets for sending, it is needed to increase duty cycle. Then it is requested to other nodes on multiple hop path to increase duty cycle. It is notify through more data flag set, whether or not packet transmission. If the more data flag set “1” , then the active period is holded in addition.



[Fig. 2] Packet transmission & ACK procedure in active state

In a receiving state, it has waiting packet for sending to children tree, when it receive packet to node. Then it sleep 3u(transmission period) later after the slot sent. Every node on the path receive packet and, it is scheduled the receiving slot. If it is back off state, the tree, which is gathering data, listen ACK packet from parent tree. It is assumed that the parameter value of simulation environment is given in Table 1 for human sensor MAC communication.

In the N2 tree level, data packet is gathered from n11 node and n12 node according to given time slot, and responded ACK packet.

$$P_{n_{21}} = P_{n_{11}(data_{rx})} + P_{n_{11}(ACK_{tx})} + P_{n_{21}(data_{tx})} \qquad (1)$$

Where P_{n21} is consumed power in node21, $P_{n11}(data_{rx})$ is received power from node11, $P_{n11}(ACK_{tx})$ is transmitted power from node21, $P_{21}(data_{tx})$ is transmitted power to node31.

In case of n41, the power consumption can be expressed as the follows in Eq(2) and Fig. 4.

In the N2 tree level, data packet is gathered from n11 node and n12 node according to given time slot, and responded ACK packet.

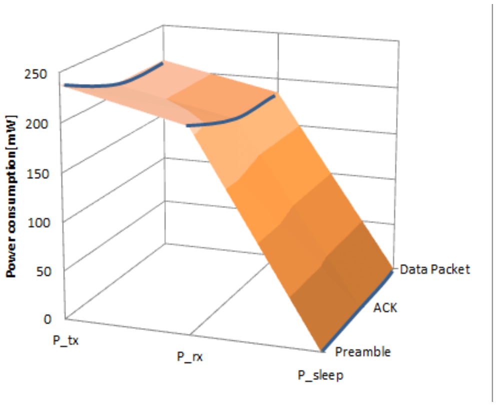
$$P_{n_{21}} = P_{n_{11}(data_{rx})} + P_{n_{11}(ACK_{tx})} + P_{n_{21}(data_{tx})} \qquad (1)$$

Where P_{n21} is consumed power in node21, $P_{n11}(data_{rx})$ is received power from node11, $P_{n11}(ACK_{tx})$ is transmitted power from node21, $P_{21}(data_{tx})$ is transmitted power to node31.

〈Table 1〉 Parameter value for convergence human sensor MAC communication

Parameter	Value
Duty cycle	10%
Listen time	18msec
Sleep time	180msec
Preamble	90bits
ACK	80bits
Transmitting I(mA)	800uA(avg.)
Receiving I(mA)	700uA(avg.)
deep sleep I(clock only)	0.8uA
Data packet	80bits

It is shown power consumption of ACK, synchronization, data packet in Fig.3.

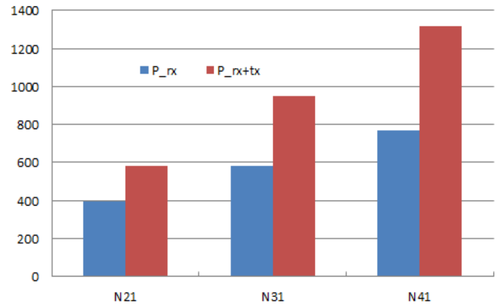


[Fig. 3] Power consumption of ACK, synchronization, data packet

In case of n41, the power consumption can be expressed as the follows in Eq(2) and Fig. 4.

$$P_{n_{41}} = P_{n_{41}(ACK_{tx})} + P_{n_{11}(data_{rx})} + P_{n_{21}(data_{rx})} + P_{n_{31}(data_{rx})} + P_{n_{41}(data_{tx})} \qquad (2)$$

If node level is increased, power consumption is increased due to upper node, which is gathered data packet of lower node.



[Fig. 4] Power consumption of data and ACK packet in each node

Therefore it is difficult to higher latency when it gets higher gathered data packets at intermediate node.

3. Security attack analysis of D-MAC protocol

3.1 Without authentication analysis in case of DoS attack

Once this collision more happens in the intermediate node, it fell throughput, which is transmission performance rate. The attacker has induced collision in the intermediate node intentionally. This is not only disturbed normal communication, but also caused to energy consumption in respect to received sink node.

In terms of network, more increasing depth of tree to upper node, it is increasing to sending data packet and duty cycle. This problem is related to denial of service attack and caused to packet collision due to little attack from attacker.

In the victim N2 level, data packet is gathered from normal n11' node and n11' abnormal node according to given time slot, and responded ACK packet. The consumed power at victim node n21 is as follows in Eq(3).

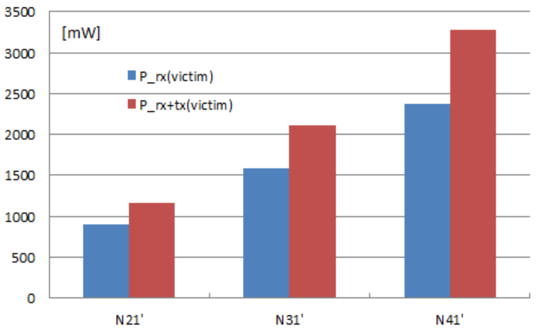
$$P_{n_{21}'} = P_{n_{11}(data_{rx})} + P_{n_{11}(ACK_{tx})} + P_{n_{11'}(data_{rx})} + P_{n_{11'}(ACK_{tx})} + P_{n_{21}(data_{tx})} \qquad (3)$$

Where $P_{n21'}$ is consumed power in victim node21, $P_{n11}(data_{rx})$ is received power from node11, $P_{n11}(ACK_{tx})$ is transmitted power from node21. $P_{n11'}(data_{rx})$ is received power from attacked node11', $P_{n11'}(ACK_{tx})$ is transmitted power to attacked node11', $P_{n21}(data_{tx})$ is transmitted power to node31.

Therefore, the consumed power at victim node n41' is as follows in Eq(4) and Fig. 5.

$$P_{n_{41'}} = P_{n_{41}(ACK_{tx})} + P_{n_{11}(data_{rx})} + P_{n_{11'}(data_{rx})} + P_{n_{21}(data_{rx})} + P_{n_{21'}(data_{rx})} + P_{n_{31}(data_{rx})} + P_{n_{31'}(data_{rx})} + P_{n_{41}(data_{tx})} \qquad (4)$$

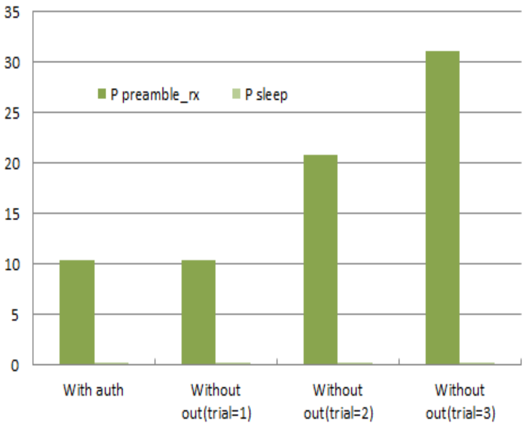
In upper intermideate node compared to lower node, it is more affected by collision attack as follows in Fig. 5.



[Fig. 5] Power consumption of data and ACK packet at victim node

3.2 With authentication analysis in case of DoS attack

In active state, it is shown that the power consumption of preamble packet between victim node and authenticated node in Fig. 6. Given in Fig.6, if authentication scheme is applied, it is related to power consumption of preamble whether or not with and without authentication process. It is reduced to energy consumption, when it is applied to authentication.



[Fig. 6] Comparison of power consumption of preamble packet between without and with authentication according to attack trail

4. Conclusion

In this paper, we present efficiency issue of power consumption according to whether or not security authentication of D-MAC in convergence network environment. Future work will take the effort to deal with security authentication scheme in convergence network environment.

ACKNOWLEDGMENTS

This paper was supported by research fund of

Industry Academia Cooperation Group of Baekseok University in 2014.

REFERENCES

[1] Eoin O'Connell, Brenda O'Flynn, David Boyle, Energy & Reliability optimal MAC for WSNs, DRCN2014, pp.1-8, 2014.

[2] Mahendra Ram, Sushil Kumar, Analytical energy consumption model for MAC protocol in wireless sensor network, SPIN2014, pp.444-447, 2014.

[3] Saylee S. Thorat, S. D. Markande, Reinvented fuzzy logic secure media access control protocol to improve lifespan of wireless sensor networks, ICICT2014, pp.344-349, 2014.

[4] Cristina Cano, David Malone, Boris Bellalta, Jaume Barcelo, On the improvement of receiver initiated MAC protocols for WSN by applying scheduling, WoWMoM2013, pp.1-3, 2013.

[5] Mouzehkesh Nesa, Zia Tanveer, Shafigh Saman, Zheng Lihong, D^2MAC: dynamic delayed medium access control protocol with fuzzy technique for wireless body area networks, BSN2013, pp.1-6, 2013.

[6] Messaoud Doudou, Mohammad Alaei, Djamel Djenouri, Jose M. Barcelo ordinas, Nadjib Badache, Duo MAC: energy and time constrained data delivery MAC protocol in wireless sensor networks, IWCMC2013, pp.424-430, 2013.

[7] Afraa Attiah, Mustafa Ilhan Akbas, Mainak Chatterjee, Damla Turgut, EE-MAC: energy efficient sensor MAC layer protocol, LCN2013, pp.116-119, 2013.

[8] Wei Shen, Tingting Zhang, Filip Barac, Mikael Gidlund, PriorityMAC: A priority enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks, IEEE transactions on industrial informatics, Vol.10, No.1, pp.824-835, Feb. 2014.

[9] Xiuming Zhu, Song Han, Pei Chi Huang, Aloysius K. Mok, Deji Chen, MBStar: A real time communication protocol for wireless body area network, ECRTS2011, pp.58-66, 2011.

[10] Vivek S. Deshpande, Dattatray S. Waghole, Performance analysis of FMAC in wireless sensor networks, WOCN2014, pp.1-5, 2014.

홍 진 근(HONG, JINKEUN)

- 1991년 2월 : 경북대학교 전자공학과(공학사)
- 1994년 2월 : 경북대학교 전자공학과(공학석사)
- 2000년 2월 : 경북대학교 전자공학과(공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 정보보호정책, 융합ICT보안
- E-Mail : jkhong@bu.ac.kr