http://dx.doi.org/10.14400/JDPM.2013.11.12.447

Security Review of B-MAC Communication Protocol

Jinkeun Hong*

Div. of Information and Communication, Baekseok University*

B-MAC통신 프로토콜에서 보안 리뷰

홍진근*

*백석대학교 정보통신학부

Abstract Berkley Media Access Control (B-MAC) protocol is one of the well-known MAC protocols, which uses adaptive preamble sampling scheme and is designed for wireless sensor networks (WSN). In this paper, we are reviewed about security vulnerability in B-MAC, and analyzed the power which is consumed at each stage of B-MAC protocol according to vulnerability of denial of sleep(DoS) and replay problem. From our analytical results, it can be considered the need of power efficient authentication scheme which provides the reliability, efficiency, and security for a general B-MAC communication. This is the case study of possible DoS vulnerability and its power consumption in B-MAC

Key Words : MAC, DoS, Security, Communication

요 약 B-MAC 프로토콜은 WSN을 위해 설계된 적용적인 프리엠블 샘플링 기법을 사용하는 잘 알려진 MAC 프로토콜이다. 이 논문에서 우리는 B-MAC 보안 취약성에 관해 살펴보았으며, 슬립 거부 공격의 취약성과 재연공격 문제에 따른 B-MAC 프로토콜의 각 단계에 소비되는 전력을 분석하였다. 연구결과로부터 일반적인 B-MAC 통신을 위한 신뢰성, 효율성, 보안을 제공하는 전력에 효율적인 인증 기법의 필요성에 대해 고찰하였다. 이 연구는 B-MAC에서 전력소비와 가능한 서비스 거부 공격 취약점에 대한 사례연구이다.

주제어 : MAC, 서비스 거부 공격, 보안, 통신

1. Introduction

Wireless sensor network is applied to a wide range of applications such as, ubiquitous computing, medical system, environmental monitoring, robotic exploration, military communication and various other fields. B-MAC use local schedule and send preamble that is slightly longer than the sleep period. But it suffers from overhearing problem. Rajesh Krishna Panta et al presents about efficient asynchronous lower power listening for wireless sensor networks in [1]. This paper reviews that early duty cycling protocols like B-MAC that were designed for bit streaming radios achieve low duty cycle by keeping the radio transceiver

Received 30 October 2013, Revised 27 November 2013
Accepted 20 December 2013
Corresponding Author: Jinkeun Hong(Baekseok University)
Email: jkhong@bu.ac.kr

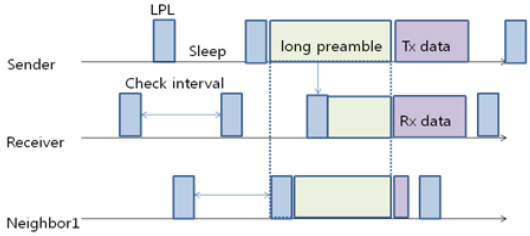
ISSN: 1738-1916

awake for short time periods. Joseph Polastre et al reviews about versatile low power media access for wireless sensor networks, and this paper show that show that B-MAC's flexibility results in better packet delivery rates, throughput, latency, and energy consumption than S-MAC in [2]. Himanshu singh et al describes about Comparison of CSMA based MAC protocols of wireless sensor networks and implemented S-MAC, T-MAC, B-MAC, B-MAC+, X-MAC, DMAC and Wise-MAC in TOSSIM, and presents the comparative study of CSMA based protocols for WSNs, showing which MAC protocol is suitable in a particular environment and supports the arguments with the simulation results in [3]. Noseong Park et al presents about a multi access asynchronous low power MAC based on Preamble Sampling for WSNs in [4]. This paper features the variable preamble interval. Because that the sampling duration must be longer than the preamble interval. Jing Li et al reviews about achievable throughput in duty cycled wireless networks. This paper abstract four schedulers, each of which represents several well-used MAC schedulers, namely sender-centric synchronous (e.g. S-MAC, T-MAC and SCP-MAC), receiver-centric synchronous (e.g. O-MAC), sender-centric asynchronous (e.g. BMAC, X-MAC and BoX-MAC), and receiver-centric asynchronous (e.g. RI-MAC), and compare throughput of schedulers in [5]. Sung Hwan Jung et al presents iterative analysis of single hop B-MAC network under poisson traffic and is reviewed service delay problem about energy consumption and poisson traffic in [6]. Giorgio Corbellini et al reviews density aware MAC for dynamic wireless sensor networks and compares DA-MAC to B-MAC and SCP-MAC in [7]. Also Giorgio Corbellini et al presents about energy evaluation of preamble sampling MAC protocols for wireless sensor networks and compares B-MAC and X-MAC to LA-MAC in [8]. At LA-MAC, this paper proposes best performance in contexts of high density and traffic congestion. Hans Christian Halfbrodt describes definition about MAC protocol such as S-MAC, B-MAC, WiseMAc, IEEE802.15.4 and X-MAC in [9]. However, the most works in wireless sensor network are focused on energy-efficient communication protocols and analysis of power consumption. These works were done insufficient in the analysis of DoS vulnerability and its power consumption caused by compromised node in wireless sensor network. In this paper, a case study about denial of sleep attack in B-MAC protocol is reviewed. For power consumption at each protocol stage, while attacking a communication between a node and its neighboring node using B-MAC protocol is analyzed and compared. This work differs from previous works in that it concentrates on one significant aspect of security vulnerability in B-MAC communication environment, namely denial of sleep vulnerability of B-MAC protocol and power consumption caused by denial of sleep attack. The analytical results can be used to design a power-efficient communication scheme for wireless sensor network security. The remaining paper is organized as follows. In section 2, we describe B-MAC communication protocol environment. Next, in section 3, we analyze the security vulnerabilities of B-MAC protocol and compare the power consumption at each stage of B-MAC protocol procedure according to denial of service attack. Finally in section 4, we review our conclusions.

2. B-MAC Communication Protocol Environment[4-5]

B-MAC is typical asynchronous protocol and is implemented CSMA based lower power consumption scheme using low power listening (LPL) algorithm, which means node listening for data transmission, and extended preamble. Like other MAC scheme, it has the period, which consists of active and sleep mode, each

node operates as independent schedule. It consists of periodic listen and sleep, frame collision and overhearing, and during short time interval, turn on the radio channel, whether there is a valid signal is checked. Each node is awaken at specified time interval in different time and determined whether the channel is being used. This process is LPL. If the preamble is detected, it is determined whether or not the receiving according to destination address. Then this preamble has a long length. The length of preamble is longer than data to transmit and receive, and consume more energy. Therefore this long preamble, which is used to transmission and receiving, is consumed a lot of energy.



[Fig. 1] Communication Procedure of B-MAC protocol

In Fig.1, B-MAC has independent check interval, and is awaken, after random time interval, which is applied a short back off algorithm, and perform LPL operation to determine whether a valid signal is present. In any node, if there is data to be sent, a check interval longer than the preamble send and notify to neighboring nodes. Then the transmitting data frame is followed. And the length of preamble is over check interval, and it has sufficiently long length, which is to be able to receive at all nodes. The neighbor node can be awakened and received preamble at random time according to check interval. The node, which is receiving preamble, may be listening to the reception of the preamble. First it observe receiver address of transmission frame followed by preamble, and if the destination is itself, it receive data while maintaining the receiving state. If destination is not his address, his node goes into sleep mode immediately.

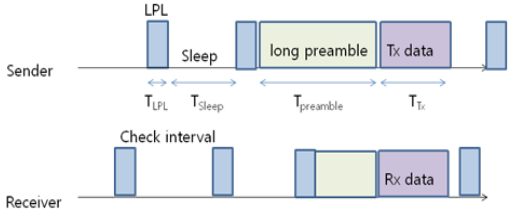
〈Table 1〉 Parameters for power consumption

Symbol	Description
T_{LPL}	Time for LPL
T_{sleep}	Time for sleep mode
$T_{preamble}$	Time for preamble
$T_{Tx-data}$	Time for transmission
$_{LRx\_data}$	Time for reception
T_{total}	Total time duration
T_{ACK}	Time for ACK
P_{LPL}	Consumed power for LPL
P_{sleep}	Consumed power for sleep mode
$P_{preamble}$	Consumed power for preamble
P_{Tx_data}	Consumed power for transmission
P_{Rx_data}	Consumed power for reception
P_{ACK}	Consumed power for ACK
L,M,N,V,W	Number of occurred iteration in given times

The power consumption in Sender can be expressed as the following in Eq(1).

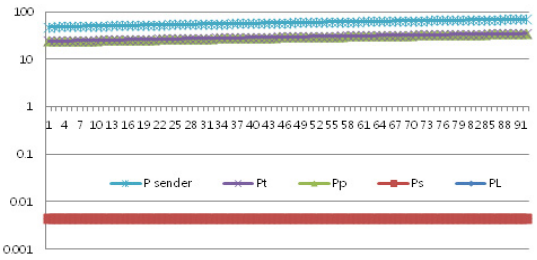
$$P_{sender} = P_{LPL}\frac{T_{LPL}}{T_{total}}L + P_{sleep}\frac{T_{sleep}}{T_{total}}M + P_{preamble}\frac{T_{\mathrm{Preamble}}}{T_{total}}N + P_{Tx-data}\frac{T_{Tx-data}}{T_{total}}V \quad (1)$$

In Fig.2, in terms of transmitting and receiving in each part, it presents the required time according to timing.



[Fig. 2] Comparison energy consumption at sender and receiver

However, most of the power, which is consumed in the process of transmitting, is power for preamble and power for Tx data.

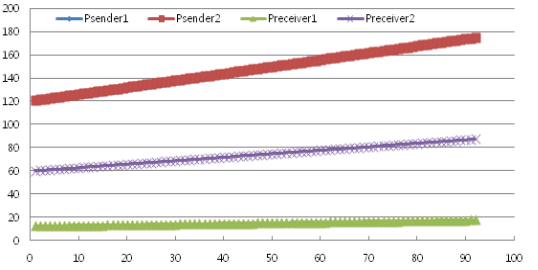


[Fig. 3] Comparison energy consumption at sender (at occurred number = 1)

According to increase the number of preamble transmission and Tx data, the consumption power is increased. Power consumption at the receiving is followed in Eq(2).

$$P_{Receiver} = P_{LPL}\frac{T_{LPL}}{T_{total}}L + P_{sleep}\frac{T_{sleep}}{T_{total}}M + P_{preamble}\frac{T_{Preamble/2}}{T_{total}}N + P_{Rx-data}\frac{T_{Rx-data}}{T_{total}}V + P_{ACK}\frac{T_{ACK}}{T_{total}}W \quad (2)$$

In the normal communication state, energy consumption presents in Fig.4. The energy consumption of sender is increased, the receiver is less.



[Fig. 4] Comparison energy consumption at sender & receiver of normal communication state (at occurred number = 1/3)

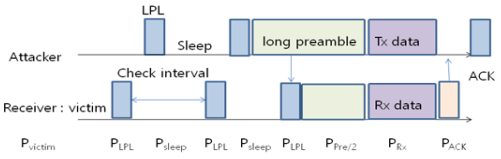
3. Security Analysis of B-MAC Communication Protocol

If the node sender communicates with receiver node, it transmits LPL and preamble packet. Received Node is respond to preamble/2 signal by asynchronous communication. If attack node target any destination node, its node is received continuously preamble and data frame, the receiving node cannot go to sleep mode and will be listening or awakening state. The receiving node is consumed power until termination of preamble and data transmission.

3.1 Abnormal state in case of DoS attack

However, it is assumed that an attacker node is much closer to the receiver node. Attacker node disguises itself as a receiver node and responds with ACK packet to sender node, there exists no countermeasure, which is tried to avoid this attack. That is, currently there is no suitable countermeasure scheme to prevent reply attack in the physical connection and authentication scheme to authenticate receiver node. Attacking sender node sends the LPL and preamble packet into receiving victim node (attacker node and neighbor node). In this case, according to denial of sleep attack, receiver node goes out to sleep mode.

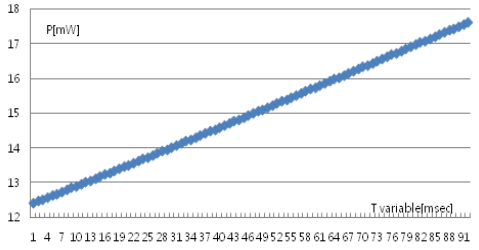
$$P_{Victim} = P_{LPL}\frac{T_{LPL}}{T_{total}}L + P_{sleep}\frac{T_{sleep}}{T_{total}}M + P_{preamble}\frac{T_{Preamble/2}}{T_{total}}N + P_{Rx-data}\frac{T_{Rx-data}}{T_{total}}V \quad (3)$$



[Fig. 5] Comparison energy consumption at attacker and victim receiver

The power of victim is as follows in Eq(4). It is assumed such that L is 3, M is 2, N is 1, V is 1 and W is 1.

$$P_{Victim} = P_{LPL}\frac{T_{LPL}}{T_{total}} + P_{sleep}\frac{T_{sleep}}{T_{total}}2 + P_{ACK}\frac{T_{ACK}}{T_{total}} + P_{preamble}\frac{T_{\Pr eamble/2}}{T_{total}} + P_{Rx-data}\frac{T_{Rx-data}}{T_{total}} \quad (4)$$



[Fig. 6] Energy consumption at P_{victim}

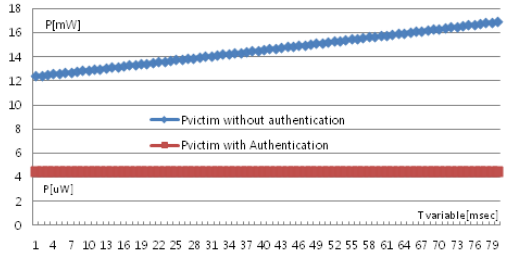
If an attacker deliberately induced the reception of data, the victim node cannot go back to sleep mode and keep awake state. Therefore the receiver power will consume excessive at the receiver victim node. The attacker deliberately transmit the long preamble to the destination, the victim node receive the preamble continuously and consume the power energy due to receive the preamble and Rx data. However the attacker deliberately transmits preamble and data to continue more, the power consumption of victim node is increased. However, since the authentication scheme is not applied to the packet exchange between the sender node and the receiver node, normal receiver is not go back to sleep.

3.2 Normal state with Authentication

If it applied authentication scheme in transmission and receiving stage, the receiver go back to sleep. Therefore the energy consumption is decreased in the receiver stage.

$$P_{Reiceiver} = P_{LPL}\frac{T_{LPL}}{T_{total}}L + P_{sleep}\frac{T_{sleep}}{T_{total}}M \quad (5)$$

In Fig.7, it compared to energy consumption according to authentication application. In case of energy consumption of victim node without authentication, the energy consumption is increased. But in the other case, which is with authentication, the energy consumption of victim node is decreased.

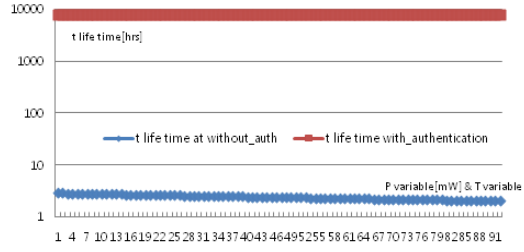


[Fig. 7] Energy consumption at normal vs. abnormal state of P_{victim}

In the respect of battery capacity, sensor residual battery lifetime B (mAh) is obtained as in Eq(6) and Fig.8.

$$Bat_{mAh} = E_{mW}\frac{T_{Lifetime}}{Vtg_{sensor}} \quad (6)$$

Given in Eq(6), life time of the victim sensor node is as follows in Fig.8. The life time of sensor node, which is not applied authentication, is short. But the life time is survival during long time.



[Fig. 8] Life time Comparison at without_auth vs. With_auth state of P_{victim}

4. Conclusion

This paper reviewed the case study of denial of

sleep attack in the B-MAC protocol. It also analyzed power consumption at each protocol stage while attacking a communication between nodes. Simulation results showed that the power consumption of communication by not using authentication and that of the communication by using authentication. This work is the analysis of security vulnerability and its power consumption caused by denial of sleep attack in B-MAC. It can be significant to the use for application of power efficient authentication and security scheme in a secure wireless sensor network.

References

[1] Rajesh Krishna Panta, James A. Pelletier, Gregg Vesonder, "Efficient Asynchronous Low Power Listening for Wireless Sensor Networks," 31st ISRDS2012, pp.291-300, 2012.

[2] Joseph Plastre, Jason Hill and David Culler, "Versatile Low Power Media Access for Wireless Sensor Networks," Sensys'04, pp.1-14, 2004.

[3] Himanshu Singh and Bhaskar Biswas, "Comparison of CSMA based MAC protocols of wireless sensor networks," International Journal of AdHoc Networking Systems, Vol.2, No.2, pp.11-20, 2012.

[4] Noseong Park, Bong Wan Kim, Yoonmee Doh and Jongarm Jun, "A Multi-Access Asynchronous Low-Power MAC based on Preamble Sampling for WSNs," IEEE ISCC2011, pp.445-450, 2011.

[5] Jing Li, Wenjie Zeng, and Anish Arora, "Achievable Throughput in Duty-Cycled Wireless Networks," IEEE 9thMASS2012,pp.290-298,2012.

[6] Sung-Hwan Jung, Nakjung Choi and Taekyoung Kwon, "An Iterative Analysis of Single-Hop B-MAC Networks Under Poisson Traffic," Journal of Communications and Networks, Vol14, Issue1, pp.40-50, 2012.

[7] Giorgio Corbellini, Emilio Calvanese Strinati, Elyes Ben Hamida and Andrzej Duday, "DA-MAC: Density Aware MAC for Dynamic Wireless Sensor Networks," 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, pp.920-924, 2011.

[8] Giorgio Corbellini, Cedric Abgrall, Emilio Calvanese Strinati, and Andrzej Duda, "Energy Evaluation of Preamble Sampling MAC Protocols for Wireless Sensor Networks," IEEE PIMRC2012, pp.387-392, 2012.

홍 진 근(HONG, JINKEUN)

- 1991년 2월 : 경북대학교 전자공학과(공학사)
- 2000년 2월 : 경북대학교 전자공학과(공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 정보보호정책, 통신네트워크보안

- E-Mail : jkhong@bu.ac.kr