한국산학기술학회논문지
Vol. 11, No. 12, pp. 4760-4765, 2010

Security Issue in T-MAC Communication Protocol

Jin-Keun Hong[1*]
[1]**Division of Information Communication, Baekseok University**

T-MAC 통신 프로토콜에서 보안 이슈

홍진근[1*]
[1]백석대학교 정보통신학부

Abstract Time out-medium access control (T-MAC) protocol is one of the well-known MAC protocols designed for wireless sensor networks (WSN), and is proposed to enhance the poor performance of the S-MAC protocol. In this paper, we are reviewed about security vulnerability in T-MAC, and analyzed the power which is consumed at each stage of T-MAC protocol according to vulnerability of denial of service (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 T-MAC communication. This is the case study of possible DoS vulnerability and its power consumption in T-MAC.

요 약 본 T-MAC 프로토콜은 WSN을 위해 설계된 잘 알려진 MAC 프로토콜이다. 본 논문에서 우리는 T-MAC 보안 취약성을 살펴보고 DoS 취약성과 재연공격에 대한 취약성과 관련하여, T-MAC 각 단계별 소모하는 전력을 분석하였다. 분석된 결과로부터 일반적인 T-MAC 통신을 위한 신뢰성, 효율성, 보안을 제공하는 전력에 효율적인 인증기법의 필요성을 고려하였다. 이 연구는 T-MAC 통신에 전력 소비 및 DoS 취약성 사례 연구에 관한 것이다.

Key Words : Security, Sensor Network, Vulnerability

1. Introduction

WSN is approached to a wide range of applications such as, environmental monitoring, medical system, robotic exploration, military communication, ubiquitous computing, and various other fields. Each node in the sensor network is a small device which is composed of one or more sensors, embedded processors, and radios. It is able to sense, gather, process distributed data and transmit to other typically over an radio channel [1- 3]. T-MAC is a MAC protocol, which is listen period ends, when no activation event has occurred in the WSN. It also has good scalability and collision avoidance capability through a combined scheduling and contention scheme like S-MAC. Another interesting problem of the protocol is that it has the ability to make trade-offs between energy and latency according to transmission conditions of the channel [1].

There have been several previous researches regarding communication protocols and security issues for WSN. W. Ye et al [1] presented SMAC, a new MAC protocol explicitly designed for WSN. In [2], a dynamic sensor MAC protocol (DSMAC) with an adaptive duty cycle has been proposed and tradeoff between power consumption and latency has been discussed. The robust and light -weight routing mechanism that can be incorporated in any routing protocol for WSN to make it fault tolerant was studied[3], and a global synchronization algorithm for WSN and several aspects of the algorithm was addressed in [4]. The energy consumption of the SMAC protocol in single-hop WSN considering an unsaturated conditions has been analyzed in [5]. T. V. Dam et al[6] suggested

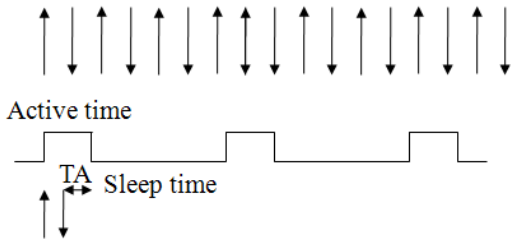
*Corresponding Author : Jin-Keun Hong(jkhong@bu.ac.kr)
Received October 18, 2010 Revised November 11, 2010 Accepted December 17, 2010

T-MAC, an adaptive energy-efficient MAC protocol for WSN that minimized idle listening. Also, fuzzy-based adaptive filtering scheme selection method [7] and unified radio power management framework [8] for energy saving in WSN were described. A robust and energy-efficient solution for secure operation of WSN was considered in [9], while a novel attack on listen-sleep MAC protocols, namely synchronization attack was presented in [10-11]. However, the most works in WSN are focused on energy-efficient communication protocols and analysis of power consumption. No work was done in the analysis of DoS vulnerability and its power consumption caused by compromised node in WSN. In this paper, a case study of DoS and replay attack in T-MAC protocol is reviewed. Its power consumption at each protocol stage while attacking a communication between a node and its neighboring node using T-MAC protocol is analyzed and compared. This work differs form previous works in that it concentrates on one significant aspect of a security vulnerability in T-MAC communication environment, namely DoS vulnerability of T-MAC protocol and power consumption caused by DoS attack. This is believed to be the analysis of security vulnerability and its power consumption caused by DoS attack in T-MAC protocol. The analytical results can be used to design a power-efficient communication scheme for WSN security. The remaining paper is organized as follows. In section 2, we describe the characteristics of T-MAC communication protocol. Next, in section 3, we analyze the security vulnerabilities of T-MAC protocol and compare the power consumption at each stage of T-MAC protocol procedure according to DoS attack. Finally in section 4, we review our conclusions.

2. Characteristics of T-MAC Communication Protocol

T-MAC tries to reduce energy consumption from various energy wasting sources such as idle listening, collision, overhearing, and control from S-MAC. The T-MAC protocol consists of periodic listen and sleep, collision, overhearing, and message passing. Periodic listen, sleep and TA: Each sensor node goes to sleep state for a specified amount of time, and then wakes up and listen to see if any other node wants to communicate with it. During sleep state, which is considered concept of TA interval, the node turns off its radio and sets a timer to wake up later. Collision avoidance: Modified protocol follows a procedure similar to that of IEEE 802.11 for collision avoidance, including both virtual and physical carrier sensing and request to send (RTS)/clear to send (CTS) handshaking scheme.

Overhearing: T-MAC protocol avoids overhearing by letting interfering nodes go to sleep after they hear an RTS or CTS packet and TA time interval. Message passing: T-MAC protocol fragments the long message into many independent small packets and transmits them in one burst. Only one RTS packet and CTS packet are used to reserve the medium for transmitting all the data packets. In Fig.1, the basic scheme of T-MAC protocol is showed. In the T-MAC, it tramsmittes message in the start time of frame. After cycle contention and waiting/listening process, RTS is transmitted. Contention time is used always, when it is not occurred collision. If the node, which is tried to transmit, is not received response during TA interval, it returns to sleep mode. When the received node is awaken, after it is retransmitted, then it go out sleep mode.



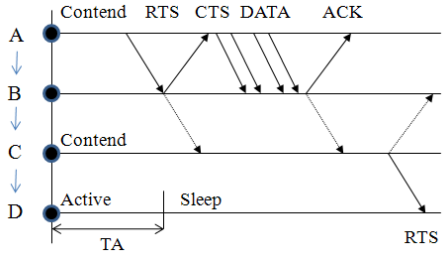
[Fig 1] Basic Scheme of T-MAC protocol

If a node keep communication with a neighbor node, it does not go sleep mode. The received time of RTS/CTS signal must be less than time of TA sufficiently. If a node is located outside of communication range, it can not be recieved RTS signal. Therefore TA interval is sufficiently longer than start time of CTS. The minimum length of TA interval shows as follows in Eq(1).

$$TA > C + R + T \quad (1)$$

Where C is contention inverval time, R is length of RTS packets, T is RTT(interval between end time of RTT and start time of CTS).

The S-MAC, which takes fixed duty cycle scheme, is not efficiently in respect of power consumption. Otherwise T-MAC is reduced power consumption in cycle of sleep mode of S-MAC. In case of S-MAC, nodes communicate with RTS/CTS awaken during sleep cycle in listen cycle. After data transmitting of nodes, they keep awaken state and inefficient in respect of power consumption. T-MAC is reduced power consumption of idle listening during active time of S-MAC. It has problem which can not be transmitted data due to transition of sleeping mode of neighbor node. In Fig 2, node C is started to contention, when communication between node C and node D is initiated. If node A and node B are transmitted data through RTS/CTS switch, node C can not be transmitted during TA interval. After transmission completion in each node A and node B, node B communicate with node C, and node C can be intiated node D. During this time, node D must be remained mode.



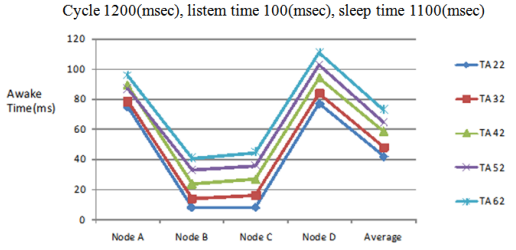
[Fig 2] Basic data exchange process

The communication environment of T-MAC is shown in Table 1.

[Table 1] T-MAC communication environment

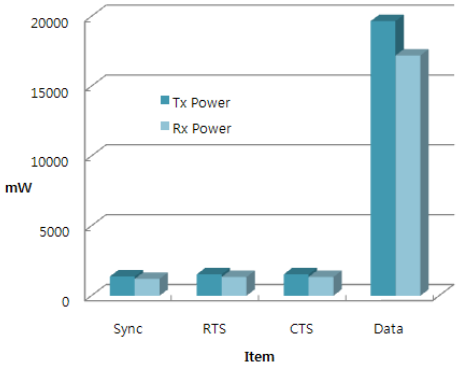
Parameter	Value
Duty cycle	10%
Listen time	150msec
Sleep time	1,500msec
Sync packet size	9Bytes
RTS/CTS/ACK	10Bytes
Transmitting current	8mA(average)
(mA)	
Receiving current(mA)	7mA(average)
Deep sleep current	8uA
Data packet size	128 Bytes
TA cycle	22~62msec
Packet cycle	1000 cycle
Packet listen interval	10 cycle(synch)

In T-MAC simulation environment, it can be assumed that cycle is 1200msec, listen time is 100msec, sleep time is 1100msec, and TA cycle is from 22mse~62msec, and simulated.



[Fig 3] Awake time in according to TA

Comparison of Tx/Rx power consumption is shown as follows in Fig 4.



[Fig 4] Tx/Rx power consumption

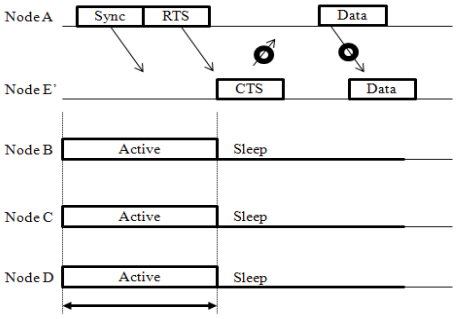
3. Vulnerability Analysis of T-MAC Protocol

If the node A communicate with other node B, C and D, it transmits Sync information and RTS packet. Received Node is respond to CTS signal. If node A wants to talk to

node B, it sends out the sync and the RTS packet. When the node B receives the sync and the RTS packet, it will reply with a CTS packet to the node A. However, it is assumed that an attacker node B' is much closer to the node A than node B. Attacker node B' disguises itself as a node B and responds with a CTS packet to node A, there exist no countermeasure which try 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 node B. Therefore, the attacker responds with a CTS packet to neighboring nodes and thus it results in disruption of the normal data transmission between sensor nodes.

3.1 Without Authentication and Replay Protection

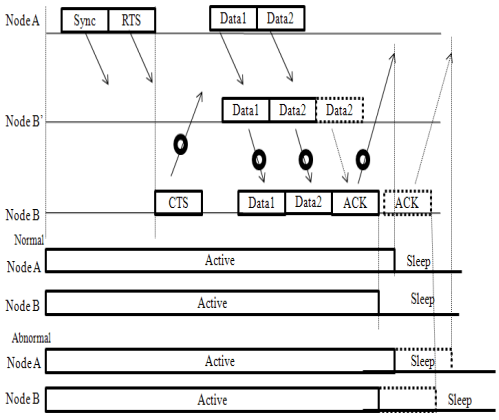
T-MAC protocol as like S-MAC is shown in Fig 5. A node A sends the sync and the RTS packet into the node E' (the near attacker), and then waits for the CTS packet from the node E'. In this case, according to DoS attack from node E', node B~D go out sleep mode, and service is denied after TA time interval.



[Fig 5] DoS attack from node E'

However, since the authentication scheme is not applied to the RTS/CTS packet exchange between the node A and the node B, the legal CTS from the node B can be accepted in the node A in Fig 6.

But it occurs delay problem of sleep time due to relayed Data2 packet from the attacker node B' which exists much closer to the node A than node B in the freshness. Therefore it occurs delayed time as much the length of data packet.



[Fig 6] Replay attack from Node B'

[Table 2] Power consumption (mW) of node A and B according to replay attack case

Node	Tx		Rx	
Node A	Sync1	1382		
	RTS1	1536	CTS1	1344
	Sync2	1382		
	RTS2	1536	CTS2	1344
	Data1	19660		
	Data1	19660		
	Data2	19660		
			ACK1	1344
Sub total		64,816		4032
Fake B'			Sync1	1209
			RTS1	1344
	CTS1	1536		
			Data1	17203
			Data2	17203
	Data2	19660		
	Data2	19660		
Node B			Sync2	1209
	CTS2	1536	RTS2	1344
			Data1	17203
			Data2	17203
			Data2	17203
	ACK1	1536		
Total		108,744		95,153

In Table 2, the power consumption of node A is 64,816mW for Tx and 4,032mW for Rx. In case of node A, it is needed to consume double power for transmission

into node B due to blocking node B'. Because of DoS attack by node B', node A retransmits Sync and RTS signal, and receives CTS signal.

[Table 3] Power consumption according to Node state

State	Tx	Rx
Normal Node A	$P_{sync}+P_{RTS}+P_{Data1}+P_{Data2}$	$P_{CTS}+P_{ACK}$
Normal Node B	$P_{CTS}+P_{ACK}$	$P_{sync}+P_{RTS}+P_{Data1}+P_{Data2}$
Abnormal Node A	$P_{sync}+P_{RTS}+P_{Data1}+P_{Data2}+P_{awaken}$	$P_{CTS}+P_{awaken}+P_{ACK}$
Abnormal Node B	$P_{CTS}+P_{awaken}+P_{ACK}$	$P_{sync}+P_{RTS}+P_{Data1}+2P_{Data2}$

Table 3 is shown the power, which is consumed at each communication stage of T-MAC protocol, as follows in Fig. 6. It will be considered consumption of the Tx and Rx power in each of normal and abnormal state. Tx/Rx power is consumed for the communication with the abnormal state, is more than that of normal state, about PData2 and Pawaken at least.

3.2 With Authentication and Replay Protection

The power of the node A during each stage is consumed less than the communication without authentication. In the transmitting process, if the authentication and replay protection is not used, the worst case of consumed power is about 203,897mW of Tx/Rx in constrained condition of simulation. In the case of communication using the authentication and replay protection, the best case of consumed power is even smaller about 49,534mW of Tx/Rx Consequently. The consumed power of the communication using the authentication scheme reduces less than, when it is compared to that of the communication not using authentication in Table 4.

[Table 4] Power consumption (mW) of node A and B with authentication and replay protection

Node	Tx		Rx	
Node A	Sync1	1382		
	Auth1	154		
	RTS1	1536	CTS1	1344
	Auth2	154	Auth3	134
	Data1	19660		
	Auth4	154		
			ACK1	1344
			Auth5	134
Sub total		23,040		2,956
Node B	CTS1	1536		
	Auth6	154		
			Sync1	1209
			Auth7	134
			RTS1	1344
			Auth8	134
			Data1	17203
			Auth9	134
	ACK1	1536		
	Auth10	154		
Total		26,420		23,114

4. Conclusions

This paper reviewed the case study of DoS attack in the T-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 DoS and replay attack in T-MAC. It can be significant to the use for application of power efficient authentication and security scheme in a secure WSN. We need to be recognize for consideration of security characteristics in each access stage of sensor mac protocol.

참고문헌

[1] W. Ye, J. Heidemann, and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks," *IEEE INFOCOM'02,* pp.1567-1576, 2002.

[2] P. Lin, C. Qiao, and X. Wang, "Medium Access Control with A Dynamic Duty Cycle for Sensor Networks," *IEEE WCNC'04,* pp.1534-1539, 2004.

[3] J. deng, R. Han, and S. Mishra, “A Robust and Light-Weight Routing Mechanism for Wireless Sensor Netowkrs,” *DIWANS'04,* 2004.

[4] W. Lee and H. S. Lee, “Analysis of a Global Synchronization Algorithm in Wireless Sensor Networks,” *IEEE MFI'08,* pp.20-25, 2008.

[5] S. Sung, H. Kang, E. Kim, and K. Kim,, “Energy Consumption Analysis of S-MAC Protocol in Single-Hop Wireless Sensor Networks,” *IEEE*, 2006.

[6] T. V. Dam and K. Langendoen, “An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks,” *ACM SenSys'03,* pp.171-180, 2003.

[7] H. Y. Lee and T. H. Cho, “Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks,” *IEICE Trans. Commun.,* Vol.E90-B, No.12, pp.3346-3353, 2007.

[8] G. Xing et al., “Towards Unified Radio Power Management for Wireless Sensor Networks,” *Wireless Communications and Mobile Computing*, Vol.9, Issue 3, pp.31-323, 2008.

[9] H. Wang, “A Robust Mechanism for Wireless Sensor Network Security,” *IEEE WiCom'08*, pp.1-4, 2008.

[10] X. Lu, M. Spear, K. Levitt, and S. F. Wu, “A Synchronization Attack and Defense in Energy-Efficient Listen-Sleep Slotted MAC Protocols,” *IARIA SECURWARE'08*, pp.403-411, 2008.

Jin-Keun Hong [Regular member]

- Dec. 2010 : Baekseok University (Div. of Information & Communication) Professor

<Research Area>
Wired/Wireless Network & Telecommunication Security, Software Security