Poster: Wormhole Attacks on Asynchronous Duty-Cycling Sensor Networks and Their Countermeasures

WenYang Wang
Department of Computer Science
Takushoku University
r48403@st.takushoku-u.ac.jp

Takashi Minohara
Department of Computer Science
Takushoku University
minohara@cs.takushoku-u.ac.jp

Abstract

Because of the open nature of the wireless communication, wireless sensor networks(WSNs) will face security issues. Wormhole attack is one of the most serious attacks against WSNs, since wormholes are created with regular routing procedure, and they are difficult to detect. Most of the proposed methods against wormhole attack assume continuous operation, so it is hard to apply them to actual WSNs which reduce their power consumption by duty-cycling operation. The duty-cycling WSNs can be classified into synchronous and asynchronous. In this paper, we focused on the wormhole attacks to asynchronous duty-cycling WSNs, and propose their countermeasures using signed acknowledgments. We have developed a prototype implementation of the attacker node and the proposed detection mechanism for the Contiki Rime protocol, and evaluated that the wormhole attacks can be detected by the adjacent nodes of the attacker.

1 Introduction

In wireless sensor networks(WSNs), the sensor nodes are required long life time with small size batteries or solar panels, so they usually work in duty-cycling operation in order to reduce their power consumption. In duty-cycling WSNs, radios of sensor nodes are stopped periodically, and any special mechanism must be used for controlling communication timing, WSNs will also face security issues because of the open nature of the wireless communication. The wormhole attack is one of the most serious attacks against WSNs, because wormholes are created with regular routing procedure. Various countermeasures against wormhole attacks are proposed[1, 3], but most of them assume continuous operation, which is not satisfied in duty-cycling WSNs. In this work, we focused on an actual behavior of WSN, and propose their countermeasures.

International Conference on Embedded Wireless Systems and Networks (EWSN) 2018
14–16 February, Madrid, Spain

ISBN: 978-0-9949886-2-1

2 Wormhole Attack to Asynchronous Duty-cycling WSNs

The duty-cycling operation of WSNs can be classified into synchronous and asynchronous categories. Time synchronization[4] between nodes is necessary for typical synchronous protocols, and wormhole attacks to synchronous WSNs will be detectable by observing delays in the synchronization phase. A variety of asynchronous duty-cycling operations are employed in MAC-layer protocols, which can be categorized into sender-initiated or receiver-initiated MAC protocols. An attacker node needs to fake the MAC protocols in either case, in order to communicate with normal nodes.

In this paper, we focus on the Contiki-MAC protocol, which is one of the sender-initiated MAC protocols, and has been implemented in a variety of sensor network hardwares with Contiki-OS[2]. As illustrated in Figure 1, which is an example packet transmission of the Contiki-MAC protocol, a sender transmits data packets repeatedly until a receiver replies with an acknowledgment or a period of transmission exceeds a sleeping interval of the receiver. The receiver, thus, can detect radio and receive a data packet when it wakes up.

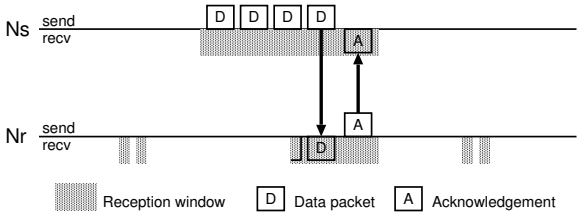

Figure 1. Example packet transmission of the Contiki-MAC

We investigated the attacks to the Contiki-MAC with assuming that a pair of attacker nodes (W1 and W2) can communicate with each other by an outbound link, and they can monitor radio continuously. There are two types of attacks to the Contiki-MAC, in which the attackers use different way to send the acknowledgments.

Figure 2 illustrates the type 1 attack, where the attacker W1 receives a data packet from a sender Ns and sends a fake acknowledgment immediately and also transfers the data packet to the corresponding attacker W2. W2 resends the data packet to the receiver Nr with using the Contiki-MAC protocol and accepts its acknowledgment.

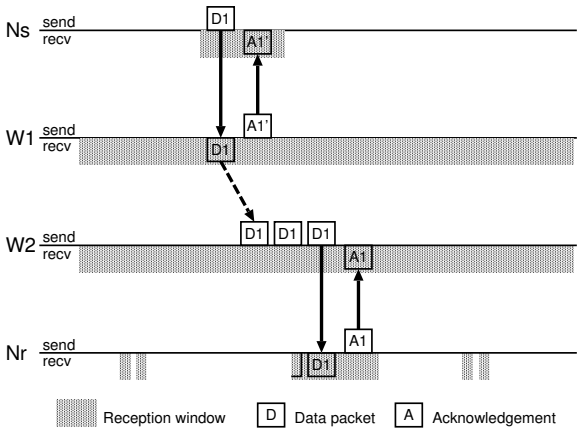

Figure 2. Type 1 attack to the ContikiMAC

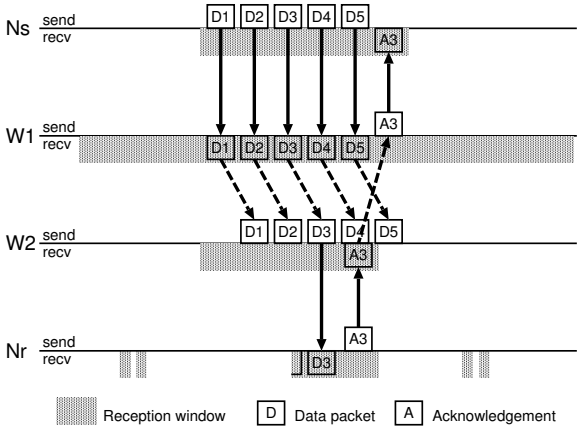

Figure 3. Type 2 attack to the ContikiMAC

Figure 3 illustrates the type 2 attack, where the attacker W1 transfers every received data packet from sender Ns to the corresponding attacker W2, and W2 resends the packets to the receiver Nr as they are. An acknowledgment packet sent by Nr is transferred through the reverse path, and replayed by W1 so that Ns can receive it.

3 Detection of the Wormhole Attacks by Using Signed Acknowledgments

In the type 1 attacks (Figure 2), the sender-side attacker arbitrarily generates acknowledgments without waiting for the receiver's responses, thus the attacker cannot reproduce the proper acknowledgments if the receiver changes them every time. We propose a challenge-response type signature attached to the acknowledgment. secret informations used for calculating a response is shared among the proper nodes in the WSN, so that each sender can examine the authenticity of the acknowledgments.

In the type 2 attacks, the sender-side attacker replays the acknowledgments received by the receiver-side attacker. And thus the challenges of the sender must be changed on every repetition of the data packets so that the acknowledgments are different for each data packe. As shown in Figure 3, the acknowledgments from attackers are delayed because they go to the other side of wormhole and return, so the sender can notice that the correspondence between a challenge and its response is not adequate.

We have developed a prototype implementation of the attacker node and the proposed detection mechanism for the Contiki Rime protocol, and conducted some evaluation with the Cooja simulator and also the Memsic's IRIS motes. The IRIS motes are equipped with 8-bit Atmel AVR ATmega128 clocked at 7.37 MHz, with 8KB SRAM and 128KB of Flash ROM, The outbound link for the wormhole is implemented on TCP connections relayed by an attacker PC using the MIB600 Ethernet interface boards (Figure 4).

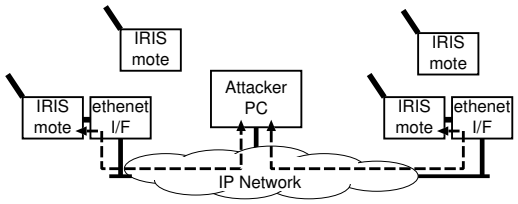

Figure 4. Implementation of a wormhole attack

We use a simple challenge-response scheme with assuming a secret value s and encryption key k are shared by sender and receiver. A sender sends message with random number r as a challenge. On receiving the message, the receiver concatenates r and s, and encrypts it with key k. Then a part of encrypted response $\{r,s\}_K$ is sent back to the sender in the Ack message. The sender also computes a response value and compares it with the response in the Ack. Although our implementation is simpler than other approaches [5], we encrypt the response value only and the burden is feasible for the motes with limited computational resources.

4 Conclusion

In this paper, we have investigated the wormhole attack to the asynchronous duty-cycling WSNs, and proposed a detection method using signed acknowledgments. Our method can detect the attacker node at the adjacent nodes and wormhole will be avoided by adding penalty cost in the route selection. The implementation of the routing for taking a detour remains as future work.

5 Acknowledgments

A part of this work was supported by JSPS KAKENHI Grant Number 25330158.

6 References

[1] D. Buch and D. Jinwala. Prevention of wormhole attack in wireless sensor netwok. *International Journal of Network Security & Its Applications*, 3(5):85–98, Sept. 2011.

[2] A. Dunkels, B. Gronvall, and T. Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *29th Annual IEEE International Conference on Local Computer Networks*, pages 455–462, Nov 2004.

[3] I. Khalil and S. Bagchi. Stealthy attacks in wireless ad hoc networks: Detection and countermeasure. *IEEE Transactions on Mobile Computing*, 10(8):1096–1112, 2011.

[4] M. Maróti, B. Kusy, G. Simon, and A. Lédeczi. The flooding time synchronization protocol. In *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 39–49, New York, NY, USA, 2004. ACM.

[5] E. K. Ryu and K. Y. Yoo. Practical techniques for ack authentication in ieee 802.15. 4 networks. *Applied Mathematics & Information Sciences*, 9(4):2169–2174, 2015.