Poster: Detection of Wormhole Attack on Wireless Sensor Networks in Duty-Cycling Operation

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

1 Introduction

Although wireless sensor networks(WSN) attracted attentions in various areas, many research challenges exist in WSN. One of the major issues WSN face is power management. In order to achieve a long life with small size batteries, wireless sensor nodes are duty-cycling, i.e. they will periodically sleep in order to reduce power consumption. Another important issue is security. Because of the open nature of the wireless communication, they are vulnerable to security attacks.

Wormhole attack is one of the most serious attacks against WSN, because wormholes are created with regular routing procedure. Various countermeasures against wormhole attacks are proposed[1, 2], but most of them assume continuous operation, which is not satisfied in duty-cycling WSN. In this work, we focused on an actual behavior of WSN, and propose wormhole detection based on delay observed in synchronized communication.

2 Time Synchronization in Duty-Cycling Wireless Sensor Networks

In most cases, WSN applications have very low data rates and do not require continuous network operation. So power cycling of sensor nodes will be the most effective way to reduce power consumption. Even though a considerable portion of power is consumed in the radio transceiver, it is difficult to power down the radio, because a node must send messages on the exact time when its peer is listening to the radio.

We assume that both synchronous and asynchronous communications are used to achieve duty-cycling operation, and every node wakes up at fixed intervals to listen for activity. When a node has a message to send, it transmits a preamble signal before the message so that its peer can notice the signal. Since the preamble of asynchronous communication must be longer than the wake-up interval time, it is less efficient than synchronous communication. So a time synchronization process on top of asynchronous communication is required to reduce the power consumption.

Many time synchronization protocols were proposed for WSN[5][3]. We assume the following synchronization protocol which distributes the system clock of the base station in a similar way used in XMesh protocol[4].

- Each node broadcasts messages which contain a time stamp measured by its own clock.
- The broadcasted message also contains an Authority Rating(AR) value. The AR represents a kind of confidence of the time stamp, and the value zero is assigned to the AR of the base station.
- The receivers adjust their clock by using the received time stamps, if the received AR is lower than their owns, and they also set their AR to the received AR + 2.

3 Proposed Detection Mechanism

Wormhole attacks are categorized into several types. In this work, we propose a method to detect the so-called stealthy attacks which will be launched by a pair of hidden collaborating nodes. One end of the wormhole overhears the packets and forwards them to the other end, where the packets are replayed to the local area. Since a wormhole forwards the packets without altering the contents, it is invisible to normal sensor nodes, and the sensor nodes near the both ends of wormhole feel themselves within only single hop distance from each other.

Our proposed method is based on the delay increased by wormhole, and consists of two parts, a detection in time synchronization procedure, and a detection in synchronized communications.

3.1 Detection by Synchronization Protocols

Figure 1 shows an example of the time synchronization process without wormhole attacks. Each node adjusts its own clock with considering the propagation delay δ, when it receives a time stamp $T(x)$ from the upstream node x. Then the receiver node y sends its time stamp $T(y)$ after some delay time $t(y)$, caused by the send/receive process, the media access and so on, is elapsed,

As shown in this example, messages for time synchronization may propagate through multiple paths. Unless any wormhole exists, the total time passed on two independent

International Conference on Embedded Wireless Systems and Networks (EWSN) 2016
15–17 February, Graz, Austria

ISBN: 978-0-9949886-0-7

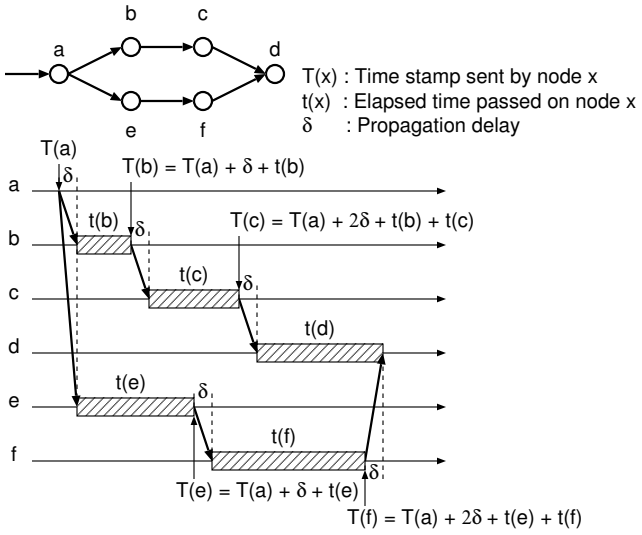

Figure 1. time synchronization with multiple propagation path

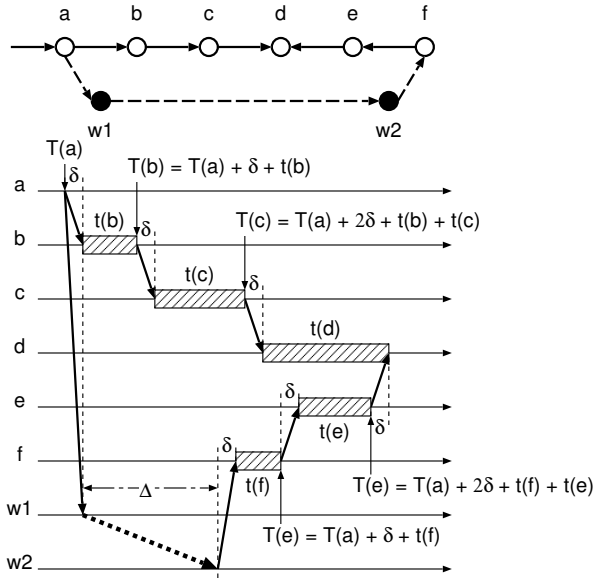

Figure 2. influence of wormhole on time synchronization

paths should match with a predictable difference;

$$3\delta + t(b) + t(c) + t(d) \approx 3\delta + t(e) + t(f)$$

Since time synchronization will be performed in flooding manner, there is a path for all propagation paths, such that the path doesn't contain a wormhole. As shown in Figure 2, the elapsed time Δ which is spent in a wormhole tunnel is not included in the total time. So we can observe a significant difference at the point where two propagation paths meet.

$$3\delta + t(b) + t(c) + t(d) \not\approx 3\delta + t(e) + t(f)$$

Furthermore, message flooding causes backwards propagation, and a node will receive time synchronization messages from its downstream nodes. If wormhole exists, the time difference observed by these reflective messages is twice as much as that in single way propagation.

In order to detect wormholes by checking the time difference, we modified the synchronization process as follows.

- Each node broadcasts messages which contain a time stamp and an AR.
- When the received AR is lower than its own AR, *the receiver node compares the time stamp with its clock, and detects wormhole if the value is too early to accept. Otherwise,* the receivers adjust their clock by using the received time stamps, and they also set their AR to the received AR + 2.
- *When the received AR is not greater than its own AR by two, the message may be reflective one, and the receiver node detects a wormhole if the time stamp is not acceptable.*

3.2 Detection by Synchronized Communication

In the synchronized communication, the message transmissions are aligned to the wake-up cycle of sensor nodes. Therefore each node must wait for the next cycle to forward a message. Even though the terminal nodes of a wormhole need not to power down the radio, they also wait for the awakening of normal nodes.

A wormhole attack pretends to provide a direct radio connection between two sensor nodes in a long distance, but it is hard to receive and forward a message at the both ends of wormhole at the same time because of the propagation delay. Thus, at least one more cycle time is added to the entire propagation time of a message. With time stamping the message at the source node, this additional delay can be detected at the base station by examining a mismatch between the hop counts and overall delay time.

4 Conclusion

In this work, we have proposed a method to detect the wormhole attacks to duty-cycling WSN based on delay observed in synchronized communication. We are implementing the proposed method on an experimental WSN consists of IRIS[4] motes, and the evaluation remains for 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] 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.

[3] 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.

[4] MEMSIC Inc., www.memsic.com. *XMesh User Manual*, 2010.

[5] E. Serpedin and Q. M. Chaudhari. *Synchronization in Wireless Sensor Networks*. Cambridge Unversity Press, 2009.