A Survey Study on Standard Security Models in Wireless Sensor Networks

Sang Ho Lee[1*]
[1]Software Engineering, Chungbuk University

Abstract Recent advancement in Wireless Sensor Networks (WSNs) has paved the way for WSNs to enable in various environments in monitoring temperature, motion, sound, and vibration. These applications often include the detection of sensitive information from enemy movements in hostile areas or in locations of personnel in buildings. Due to characteristics of WSNs and dealing with sensitive information, wireless sensor nodes tend to be exposed to the enemy or in a hazard area, and security is a major concern in WSNs. Because WSNs pose unique challenges, traditional security techniques used in conventional networks cannot be applied directly, many researchers have developed various security protocols to fit into WSNs. To develop countermeasures of various attacks in WSNs, descriptions and analysis of current security attacks in the network layers must be developed by using a standard notation. However, there is no research paper describing and analyzing security models in WSNs by using a standard notation such as The Unified Modeling Language (UML). Using the UML helps security developers to understand security attacks and design secure WSNs. In this research, we provide standard models for security attacks by UML Sequence Diagrams to describe and analyze possible attacks in the three network layers.

Key Words : Security, Wireless Sensor Networks, Unified Modeling Language, Standard Attack Models

1. Introduction

Wireless Sensor Networks (WSNs) are exploding in popularity. Major application areas include the military battlefield surveillance and civilian applications include industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, health-care applications, home automation, and traffic control [1]. Wireless sensor nodes in WSNs sense temperature, motion, sound, and vibration [2], and most WSNs are deployed in a hostile area or public outdoor area. Because of the well-known constraints of WSNs such as a limited physical size, security algorithms in a conventional networking environment are not applicable in WSNs except adding extra hardware equipment. Recently, many researchers have developed security algorithms to fit into WSNs based on descriptions and analysis of security attacks [3] [4] [5]. To better analyze security attacks and develop counter attacks, a standard security notation must be developed and provided for security developers. The well-known modeling methodology is Unified Modeling Language (UML) [6]. UML is a standard notation for the modeling of real-world objects as a first step in developing an object-oriented design methodology, and is used as the language for specifying, visualizing and constructing the artifacts of software systems. In addition, UML represents a collection of the best engineering practices that have proven successful in the modeling of large and complex systems. The key

Received 2014-10-25 Revised 2014-11-08 Accepted 2014-11-15

[*]Corresponding author: Sang Ho Lee (shlee@chungbuk.ac.kr)

benefit of using UML is that it provides security developers standardized methodologies for visualizing security attacks that are present in WSNs. However, no research has been published that uses a standard notation for security attacks. Therefore, in this research paper, we propose and present UML Sequence Diagrams for possible attacks in the three different network layers: a physical, link, and transport layer. These UML models are designed to help increase security developers' understanding as they build more secure WSNs.

The rest of this paper is organized as follows. Various attack strategies are investigated and categorized in terms of network layers in Sections II, III, and IV, respectively. Finally, in Section V we conclude the paper with future directions.

2. PHYSICAL LAYER: JAMMING AND TAMPERING

Major responsibilities in the physical layer are signal detection, modulation, data encryption and decryption, and frequency selection [7]. Because of the use of radio signals, jamming attacks may occur in the physical layer. In addition, nodes may tend to be exposed in hostile or insecure environments where an attacker can access the nodes easily [8]. These two possible attacks, jamming and tampering, are described in Fig. 1 and Fig. 2

2.1 Jamming Attack

In a Jamming attack, a malicious node is supposed to identify the radio channel so it can disrupt the entire network with the jamming sources that are randomly distributed in the network, for example, when the malicious node 1 controlled by the attacker in Fig. 1 sends Hello signals to its neighbors with a strong powerful transmitter. If the signal of malicious node 1 is valid, then all neighbors surrounded by the malicious node 1 listen and receive the Hello signal. The detailed processes are as follows and also in Fig. 1:

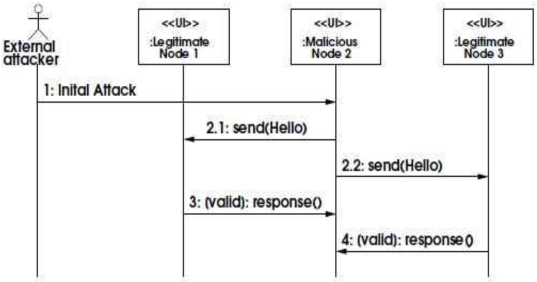

Fig. 1. UML Sequence Diagram for Jamming Attack.

1) An attacker initiates a malicious node to send its neighbor nodes a Hello message by using a radio signal, which is sharing with legitimate nodes.
2) A malicious node sends a Hello message to its neighbor nodes by using a radio signal.
3) Each node verifies the message by checking its radio channel which is shared by all legitimate nodes. If the radio signal is different from the legitimate nodes, then they simply discard the message. Otherwise, this attack will be successful.
4) The received nodes respond to the malicious node with ACK. Whenever they receive Hello messages from their neighbor, they update the table with their node identifications.

In the meantime, the neighbor nodes are controlled by the malicious node’’s signals. Jamming is a type of denia-lof-service (DoS) attack. To prevent Jamming from attackers, Frequency-Hopping Spread Spectrum (FHSS) [9] [10] is a possible solution. FHSS is transmitting signals by switching a carrier among many frequency channels using a pseudo random sequence known to both sender and receiver [8]. Without knowing the frequency selection sequence, an attacker may have difficulty jamming the radio frequency. However, the use of a wide section of the frequency band will not prevent a successful attack.

2.2 Tampering Attack

Another attack in the physical layer is a tampering attack described in Fig. 2. An attacker can access the nodes physically because most WSNs tend to be deployed in a hostile or insecure area. The attacker may extract sensitive information such as a pre-distributed key or node identification from a compromised node, which the attacker controls. In this case, the attacker can easily spoof the radio frequency channel and disrupt the entire network even though encrypted radio signals are being used. Two defenses involve tamper-proofing the nodes physical package and hiding nodes in more secure locations. However, due to the well-known constraints in WSNs, most WSNs are not tamper-proofed [8]. The detailed processes are in Fig. 2 and as follows:

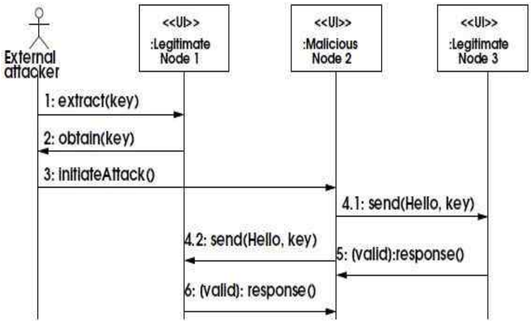

Fig. 2. UML Sequence Diagram for Tampering Attack.

1) An attacker extracts sensitive information by accessing a node 1 physically.
2) The attacker alters or replaces to create a compromised node 2 which the attacker can control.
3) The malicious node 2 sends its neighbors Hello messages to update their routing tables.
4) The neighbor nodes respond to the malicious node 2 with ACK.
5) Whenever nodes receive Hello messages from their neighbors, they update the table with their node identifications.

3. DATA LINK LAYER: COLLISION, RESOURCE EXHAUSTION, AND UNFAIRNESS

Medium access control (MAC) layer performs carrier sensing and packet transceiving. MAC protocol primarily coordinates nodes to access a wireless medium and resolves a conflict when more than two nodes compete to access the shared medium. In MAC protocol, two or more interfering nodes are not allowed to transmit packets at the same time to avoid a collision. In the presence of collision, however, MAC protocol resolves it by using a contention resolution algorithm such as resending the packet later at a randomly selected time or simply discarding the packet and leaving the retransmission to the upper layer. There are three major attacks in data link layer: collision, resource exhaustion, and unfairness.

3.1 Collision Attack

To reduce a collision due to the hidden terminal problem, two-way Request-to-Send (RTS) and Clear-to-Send (CTS) handshake is used to reserve a channel before transmitting any data packet in IEEE 802.11-based MAC protocols as shown in Fig. 3. When a node, n2, senses an event or has data to send, it selects a random backoff value from range [0, CW], where CW is contention window. The CW is decremented only when the channel is idle. When it becomes zero, n2 sends a RTS to reserve the channel for the duration of transmission. When n3 receives the RTS, it replies with a CTS to the sender after a short inter frame space (IFS) interval. Any node who overhears either RTS or CTS (e.g. n1 and n4) should defer its transmission when the medium is busy and set/update its network allocation vector (NAV) based on the duration specified in RTS/CTS. The NAV contains an expected time and indicates the remaining time of following transmission sessions, and it always decreases regardless of the medium state while the backoff decreases only when the medium is idle. After the RTS/CTS exchange, n2 sends a Data and receives an ACK from n4, if the transmission is successful.

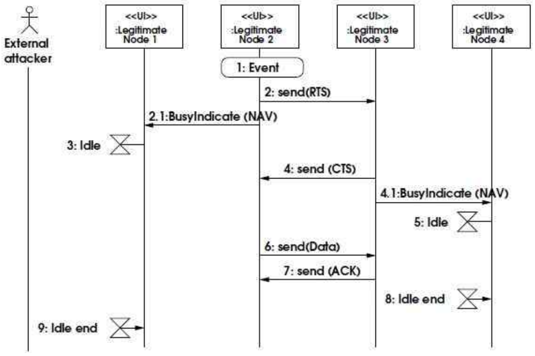

Fig. 3. UML sequence diagram of IEEE 802.11 distributed coordination function (DCF) in data link layer.

Regardless of this collision avoidance effort, a malicious node may interrupt an on-going communication by transmitting a packet simultaneously. It causes a collision and in particular the malicious node targets ACK packet to maximize the expenses in terms of communication delay and energy consumption, i.e. retransmission after an exponential back-off. Various error correcting code techniques can be used to defend this collision attack, but it may incur additional computation and communication overhead in resource limited WSNs. Also reactive jamming attack [11], [12] is similar to the collision attack, in which an attacker keeps quiet when the channel is idle but transmits a jam signal whenever it senses traffic on the channel. It is hard to detect the attacker (if it is not impossible) because it looks like a normal packet collision.

3.2 Resource Exhaustion Attack

Since wireless communication could be responsible for more than half of energy consumption [13], repeated aforementioned collision attacks by a malicious node cause a series of retransmitting control and data packets and result in battery depletion. Although a great deal of effort has been devoted to develop energy efficient MAC protocols, in which they primarily focus on how to judiciously place the radio in lowpower or sleep mode1 as long as possible without degrading the communication performance, they are quite vulnerable for resource exhaustion attack. For example, denial-of-sleep (DoS) attack [14], [15] keeps the radio in active mode[1]. A malicious node may repeatedly send a RTS for eliciting multiple CTS replies from a target and its neighbor nodes and thus, a set of involved nodes will eventually exhaust the energy. In order to prevent unnecessary energy spending, a MAC admission control can either limit a number of same requests or ignore the excessive requests. However, due to the inherent promiscuous overhearing behavior, a set of nodes still wastes energy for such a bogus RTS.

3.3 Unfairness Attack

Due to the lack of coordination, most of the MAC protocols heavily rely on a distributed contention resolution mechanism to ensure fair share of the channel. However, the implicit assumption of this mechanism is that all the nodes participating in a network follow/cooperate the protocol. Thus, a malicious node may intentionally misbehave by ignoring the protocol to obtain unfair share of the channel [16]. For example, it either selects the backoff value from a smaller range (e.g. [0, CW 4]) or uses a different backoff scheme instead of exponential backoff. Also it specifies higher transmission duration than that of actual in RTS and delays its neighbor nodes for competing the channel. These simple yet effective unfairness attacks significantly degrade the communication performance of well·behaved nodes.

4. TRANSPORT LAYER: FLOODING AND DESYNCHRONIZATION

The transport layer is primarily responsible for

[1] As pointed in [12], the Crossbow Mica2 consumes 36.81 mW in receive mode while 0.048 mW in sleep mode. It works over 4,000 days in sleep mode but only 10 days in receive mode under the two standard 3,000 mAh AA batteries.

managing end-to-end connections, and it optimally provides services including reliable data communication, flow control, congestion control, etc. Most attacks in the transport layer target the TCP/IP protocol, which is popularly deployed in current networks. There are two major attacks: flooding and desynchronization.

4.1 Flooding Attack

Flooding attacks primarily exploit weaknesses in communication protocols, where connection information must be maintained at both ends of a connection. These protocols become vulnerable when a malicious node repeatedly transmits connection request packets and attempts to exhaust resources. For example, the transmission control protocol (TCP) is a connection oriented communication protocol, which requires that a connection be established through the three-way handshake process[2]. In the TCP SYN attack [17], a malicious node can send the server multiple connection establishment requests with spoofed source addresses. This causes the server to keep allocating resources for bogus connections. When the maximum half-open connection limit is reached, any successive legitimate connection request is refused.

One of defense mechanisms is that each node demonstrates its legitimacy of connection request by solving a puzzle [18]. The server generates and verifies the puzzle, and clients should solve and show it before establishing a connection. Although this approach prevents the malicious node from quickly wasting the resource, it requires a non-negligible computational power and thus it should not be directly applied to WSN, which is a resource-limited network.

4.2 Desynchronization Attack

A malicious node can interrupt an on-going connection by repeatedly transmitting forged packets containing sequence numbers or control flags to the victims, resulting in a desynchronization between the two ends of the nodes. Then the node requests the retransmission of missed frames, resulting in resource exhaustion. If the malicious node can maintain correct timing, it can even prevent the exchange of any further packets between two ends of the nodes. This can be avoided all the packets exchanged being authenticated so that the malicious node cannot spoof the packets. In addition, packet authentication also requires a non-negligible computational power.

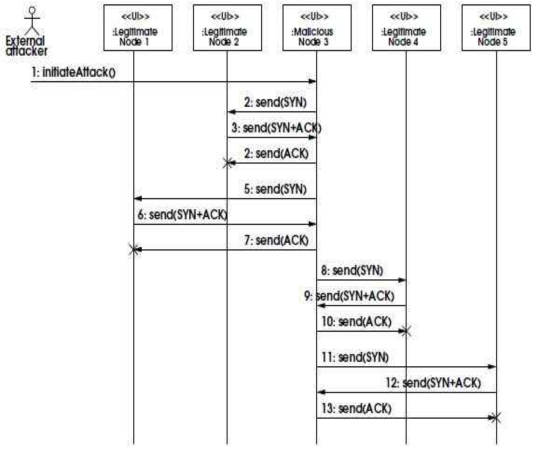

Fig. 3. UML sequence diagram of flooding attack.

5. CONCLUDING REMARKS AND FUTURE WORK

Applications in WSNs are widely spreading to surveillance operations in military or industrial process monitoring and control. In miliary applications, security is a major concern due to the characteristics of WSNs, whose wireless sensor nodes tend to be exposed by enemies. To protect WSNs from attackers, security attacks must be well analyzed so that countermeasures can be found. If we can better understand and analyze the attacks, we have a good chance of finding solid

[2] In the process, a sender sends a SYN packet to initiate a connection. A receiver replies with a SYN+ACK packet indicating that the receiver agrees the connection. Finally, the sender replies an ACK packet indicating that the connection has been established.

solutions. However, there is no current research that describes and analyzes the current attacks with standard notations. Therefore, in our research, we proposed using UML as a standardized modeling language to describe and analyze the current attacks and countermeasures. These standard models of current attacks and countermeasures are able to help increase security developers' understanding and pave the way for building more secure WSNs. In the future, we will use various UML diagrams – an activity diagram, state machine diagram, class diagram, composite structure diagram, and interaction diagram – to analyze the current attacks and countermeasures in a sophisticated way. Security measurements of the countermeasures in WSNs are still under investigation.

REFERENCES

[1] S. Hadim and N. Mohamed, "Middleware: Middleware Challenges and Approaches for Wireless Sensor Networks," IEEE Computer Society, vol. 7, no. 3, Mar. 2006.

[2] K. Romer, F. Mattern, and E. Zurich, "The Design Space of Wireless Sensor Networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 54-61, Dec. 2004.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in Proc. of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May. 2003.

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, Sep. 2002.

[5] Q. Hu, D. L. Lee, and W. Lee, "Performance Evaluation of a Wireless Hierarchical Data Dissemination System," in proc. ACM MOBICOM, 1999, pp. 163 - 173.

[6] M. Fowler, UML Distilled: A Brief Guide to the Standard Object Modeling Language (3rd ed.). Addison-Wesley, 2003.

[7] L. Akyyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[8] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, 2006.

[9] J. C. Haartsen and S. Mattisson, "Bluetooth-A New Low-Power Radio Interface Providing Short-Range Connectivity," in Proc. of the IEEE, pp. 1651 - 1661, Oct. 2000

[10] J. Haartsen, "The Bluetooth Radio System," IEEE Personal Communications, vol. 7, no. 1, pp. 28 - 36, Feb. 2000.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in Proc. MobiHoc, pp. 46-57, 2005.

[12] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," Pervasive Computing, pp. 74 - 81, 2008.

[13] R. Kravets and P. Krishnan, "Power Management Techniques for Mobile Communication," in Proc. IEEE MOBICOM, pp. 157-168, 1998.

[14] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-Service Attacks on Battery-powered Mobile Computers," in Proc. PerCom, pp. 309 - 318, 2004.

[15] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of Denial of Sleep Attacks on Wireless Sensor Newtork MAC Protocols," in Proc. Workshop on Information Assurance, pp. 297-304, 2006.

[16] P. Kyasanur and N. H. Vaidya, "Detection and Handling of MAC Layer Misbehavior in Wireless Networks," in Proc. DSN, pp. 173-182, 2002.

[17] C. L. Schuba, I. V. Krsul, M. g. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a Denial of Service Attack on TCP," in Proc. IEEE Symposium on Security and Privacy, pp. 208 - 223, 1997.

[18] T. Aura, P. Nikander, and J. Leiwo, "DOS-Resistant Authentication with Client Puzzles," in Proc. Security Protocols Workshop, pp. 170 - 177, 2000.

저 자 소 개

이 상 호(Sang Ho Lee) [정회원]

▪ 1981년 3월 ~ 현재 : 충북대학교 전자정보대학 소프트웨어학과 교수

<관심분야> : 네트워크 보안, 개인정보보호, 데이터베이스 보안