UML Modeling of Physical and Data Link Layer Security Attacks in WSN

S N Uke
Department of Information Technology,
SKNCOE, Pune, India

A R Mahajan, PhD.
Professor & HoD,
CSE Department,
PIET, Nagpur, India

R C Thool, PhD.
Professor & HoD,
Department of Information Technology,
SGGS, Nanded, India

ABSTRACT

Wireless sensor networks (WSNs) are growing extremely and becoming more and more attractive for a variety of application areas such as surveillance of information, industrial secrets, air pollution monitoring, area monitoring, and forest fire detection, home automation, industry monitoring, and many more. As WSN is mostly used for gathering application specific information from the surrounding environment, it is highly essential to protect the sensitive data from unauthorized access. WSNs are vulnerable to various security attacks because of broadcast nature of radio transmission. The primary weakness shared by all wireless application and technologies is the vulnerability to security attacks/threats. The performance and behaviour of a WSN are vastly affected by such attacks. In order to be able to better address the vulnerabilities of WSNs in terms of security, it is important to understand the behaviour of the attacks.

This paper aims at addressing behavioral modeling of critical security attack residing in the physical layer and data link layer of wireless sensor network. UML gives the finest diagrammatic representation of any system which is best for developers. Our efforts to synchronize WSN with UML are discussed in the paper. The security attacks are modeled by using state machine diagram of Unified Modelling Language (UML). This modeling of security attacks will help programmers to develop counter measures.

General Terms

Wireless Sensor Network

Keywords

Wireless sensor networks (WSNs), Physical layer, data link layer, unified modelling language (UML), state machine diagram, security and attacks.

1. INTRODUCTION

A WSN consists of a number of small nodes, equipped with sensors, which together form a network that can perform tasks by communicating with each other using a radio. WSNs have been used in many applications like military, homeland security, machine health monitoring, environment and habitat monitoring, health-care applications, home automation, and traffic control[1] etc. Security is critical for such networks. So to make system more secure against the attacks, the knowledge of how the attacks are occurred on the network is required. Theoretical concepts can be easy to understand, but the diagrammatic representation is easier. UML is better way to represent these attacks. The Unified Modeling Language (UML) is chosen for better analysis of behavior of security attacks. UML is a well-known modelling methodology and is a standard notation of real-world objects as a first step in developing an object-oriented design methodology. It is used as the language for specifying, visualizing and constructing the artifacts of the system. UML represents a collection of the best engineering practices that have proven successful in the modelling of large and complex systems. The important benefit of UML is that it provides security developers standardized methodologies for visualizing security attacks that are present in WSNs[2]. Little research has been done in UML modelling of a WSN environment especially concerning the security. This paper proposes behavioural modelling of WSN security attacks using state machine diagrams. It will be useful to implement secure WSN.

The remainder of this paper is organized as follows: Section 2 presents behavioral modeling of physical layer attacks. Section 3 presents behavioral modeling of data link layer attacks. Finally, in Section 4 the paper concludes with future directions.

2. BEHAVIOURAL MODELLING OF PHYSICAL LAYER ATTACKS

2.1 UML Modeling

UML is a language for specifying, visualizing, constructing, and documenting the artifacts and is used to evolve and derive the system. It presents a standard way to show interactions/behaviour within the system that provides a conceptual understanding of system functionality. The UML provides a large set of diagrams such as use case diagram, class diagram, sequence diagram, activity diagram, state machine diagram, component diagram, deployment diagrams and many more to model the system behaviour.

The focus of this paper is to use UML to model security attacks using state machine diagram. A state machine diagram models the behaviour of a single object, which specify the sequence of events that an object goes through in response to events during its lifetime.

2.2 Modeling of Security Attacks

Many attacks target physical layer as all upper layer functionalities rely on it. Adversaries can do “non-technical” things such as destroying sensors, or conduct “technical” actions such as wiretapping [3]. In general, the following three types of attacks are categorized as physical layer attacks:

- Jamming Attack
- Device Tampering
- Eavesdropping

2.2.1 Jamming Attack

Jamming is one type of active attack. Active attacks are responsible for modification of the data stream as well as creation of the false data stream. Jamming attacks disrupt the availability of transmission media. The communication between sensor and nodes is interrupted by jammer or open wireless environment is interfered using radio frequencies. The loss of some crucial message may destroy the entire system [4]. Jamming attacks can be mounted from a location remote to the target networks. [5]

Jamming can be described with four types:

1) Constant jamming

It emits the constant noise. Noise can be the radio signals or random bits. The signals can be implemented using wave form generator and continuously send on network. Random bits are continuously sent by any normal wireless device without following any MAC layer protocol [5]. MAC protocol allows valid nodes to send out packets only when the channel is idle. Fig. 1 shows the behavioural modelling of constant jamming attack.

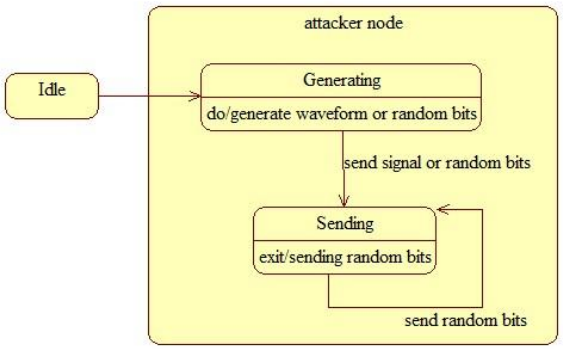

Figure 1. State machine diagram for Constant jamming attack

The details of constant jamming attack are as follow:

- Initially system in "Idle" state.
- System transit from "Idle" to "attacker node" state as attacker generates the waveform or radio signal or random bits.
- The attacker node sends the continuous signal or random bits on network, after some time network jam.

2) Deceptive jammer

Here the jammer replace the valid signals or fabricate the signals instead of sending the random bits or signal. Without any gap between packet transmissions, it constantly injects regular packets to the channel.

Fig. 2 shows behavioral modeling of Deceptive jamming attack. The details of deceptive jamming attack are as follow:

- Initially system in "Idle" state.
- Attacker node access the packet, from where the valid transmission is going on. This state of attacker node is nothing but "hacking" state.
- Once the attacker node got the packet, attacker is annoying to modify the data, which is named as "fabrication".
- Then it sends the modified data to receiver node.

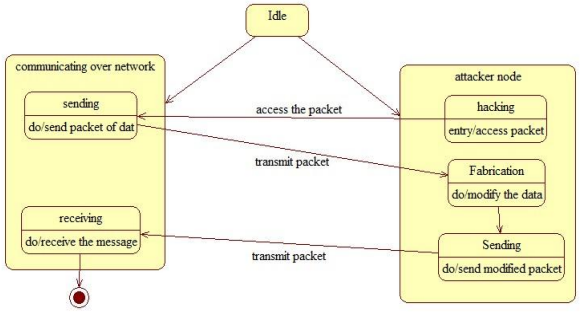

Figure 2. State machine diagram for Deceptive jamming attack

Diagram represents the state "communicating over network" described valid communication between sender node and receiver node. When the attack occurs, instead of going to the valid receiver node packet goes to attacker node. And at last receiver get the incorrect data.

3) Random jammer

Random jammer sleeps for random amount of time and jams the network for random amount of time. So instead of sending continuous signal or replacing the data, a random jammer alternates between sleeping and jamming. But it acts like constant jammer or a deceptive jammer after jamming phase and it is in sleeping mode. It turns off its radio and it goes in the sleeping mode for some time duration.

This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. [5].

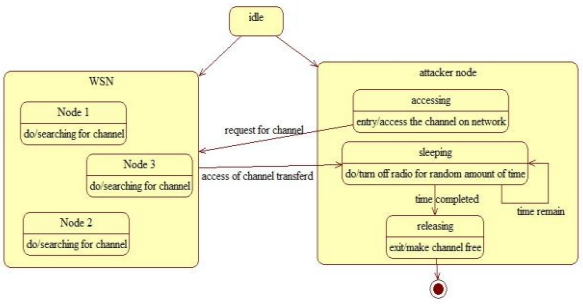

Figure 3. State machine diagram for random jamming attack

Fig. 3 shows the behavioral modeling of random jamming attack. In this attack, there is not any direct connection with the node. Attacker is interested in the channel which is used for communication purpose. Attacker node access the channel and goes into sleeping mode, every valid node in the network is then searching for channel and goes into waiting state.

- Initially system in "Idle" state.

• From "Idle" state, it switches to next state where "accessing" is sub state. In this the attacker node is accessing the channel.

• Once attacker node got the channel, it goes into sleeping mode for random amount of time.

• "Sleeping" is the sub state of attacker node state where it switches off radio signal.

• Attacker node remains in the system until the time duration is not completed.

• It releases the channel after completion of the time of sleeping.

4) Reactive jammer

Fig. 4 shows the behavioral modeling of reactive attack. They always try to block the channel irrespective of the traffic pattern of the channel. Active jammers are keeping channel busy all the time. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. Reactive jammers are harder to detect. [5]

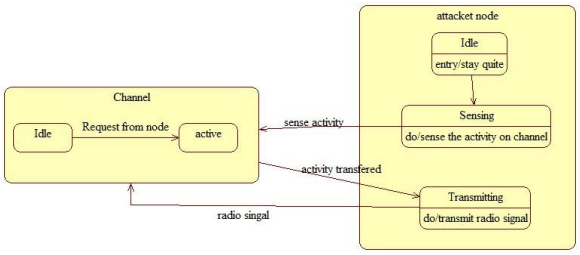

Figure 4. State machine diagram for reactive jamming attack

The details of reactive attack are as follow:

• "Idle" sub state of the "attacker node" represents that node doing nothing but it is present.

• Next state of attacker node is "sensing", represent the sensing activity of attacker node. The attacker finds that channel is in active mode or not.

• Attacker node is in "Idle" state, it stays quite.

• Attacker sense that whether the channel is in active mode or not.

• If the channel is in active mode, it senses that activity.

• Then it transmits the radio signal to channel.

2.2.2 Device Tampering

Tampering is again one of the attacks on physical layer. An attacker gets the physical access of the node so he can access or extract sensitive information like, encryption decryption keys or other data on the node. Sometimes the node can be replaced or modified by the attacker, so whole control of the node goes to the attacker.

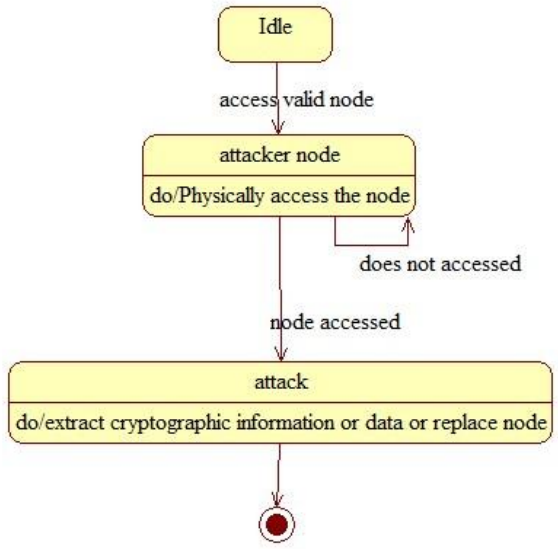

Figure 5. State machine diagram for tampering attack

Fig. 5 shows the behavioral modeling of tampering attack. Tampering attack is very easy to understand. Attacker node physically accesses the valid node and extracts the information like encryption keys, decryption keys or data. Sometimes it may replace the node.

The details of tampering attack are as follow:

• Initially object is in "Idle" state.

• Attacker node physically access valid node.

• If the node accessed, attacker node attacks on that node.

3. BEHAVIOURAL MODELLING OF DATA LINK LAYER ATTACKS

In general, the following three types of attacks are categorized as data link layer attacks:

• Collision

• Traffic Analysis

3.1 Collision

In this attack, the attacker finds out the frequency of its radio which is transmitting on WSN. After this, actual messaging is started. While sending message, it sends out its own signal interfering with the message. This is nothing but collision. The main purpose of collision is to pass the incorrect message to receiver. In theory, causing a collision in only one byte is enough to create a CRC error and cripple the message [6]. Basically the collision happens when there are two nodes which attempt to transmit the message at same frequency simultaneously. When collision is occurred there is a change in stream of data. Power consumption is less and it is hard to detect [6].

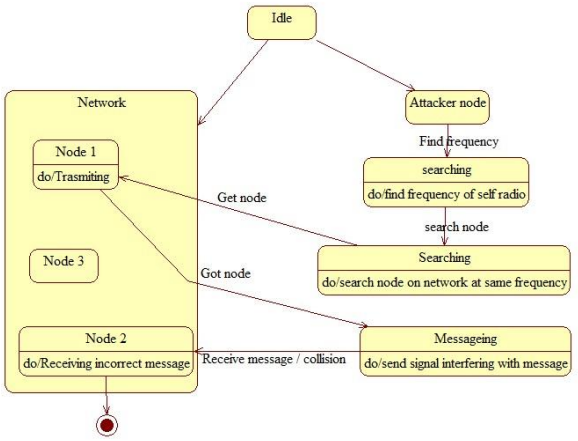

Figure 6. State machine diagram for collision attack

Fig. 6 shows the behavioral modeling of collision attack. Diagram contains two searching states. First "searching" state describes that the attacker node searches the frequency of self radio and second describes that the attacker node search for valid node at same frequency over network. At last after "Messaging" state, collision occurs. The "Network" state represents different nodes that are present in the network and the nodes who are communicating with each other.

The details of collision attack are as follows:

- Initially system in "Idle" state.
- Attacker node finds the frequency of self node.
- Attacker then finds the valid node at the same frequency on network.
- At the end the signal is interfering with message.

3.2 Traffic analysis

It is type of passive attack. It always tries to deduce the traffic pattern based on the eavesdropped information [8]. WSN is network of packets and the base stations. Packets can be transmitting to the nodes over network. There is a path between nodes which is used for addressing the node. Attacker analyze the packet traffic i.e. transmission of the packets from one node to another node and then begin with the active attacks on that location.

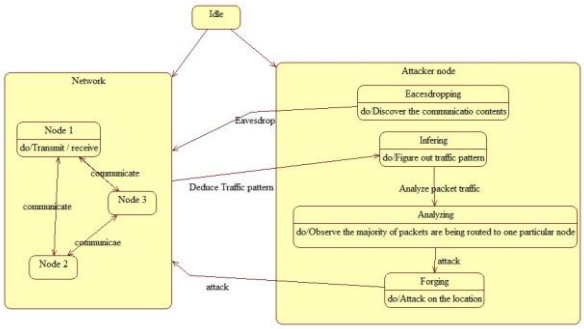

Figure 7. State machine diagram for traffic analysis attack

Fig.7 shows the behavioral modeling of traffic analysis attack. "Eavesdropping" state describes that the attacker node find the communication contents over the network. State "inferring" describes the attacker figure out the traffic pattern. Traffic pattern contains valid nodes and the communication paths between them. "Analyzing" phase describes that the attacker node find, on which route majority of packets transmitted. And at the last the "Forging" state describes that the attacker attack on that location.

From fig. 7, list of the activities by attacker node

- Eavesdropping (Discover the communication contents).
- Inferring (Figure out the traffic pattern).
- Analyzing (Observe the majority of packets being routed to one particular node).
- Forging (Attack on that location)

4. CONCLUSION

To protect WSNs from attackers, security attacks must be well analyzed. It will help to develop countermeasures. Behavioral Modeling of Physical and Data Link layer attacks on WSN with the help of state machine diagram gives the overall structure. It gives basic idea of attack occurrences. State machine diagram depict the various states that an object goes through and the transitions between those states. It will definitely give concrete solution for developing countermeasures. Some research is already done with sequential and activity modeling. This paper proposes the behavioral modeling which describes how exactly attack occur on respective layer of WSN. In future, we will analyze the behavioral modeling of attacks on other layers of WSN as well as we will create the various UML diagrams for WSN attacks such as class diagram, component diagram, deployment diagram to analyze the current attacks and countermeasures in a sophisticated way.

5. REFERENCES

[1] Sunghyuck Hong and Sunho Limt "Analysis of Attack Models via Unified Modeling Language in Wireless Sensor Networks: A Survey Study."

[2] OMG (February 2009). "OMG Unified Modeling Language (OMG UML)", Superstructure Version 2.2". http://www.omg.org/spec/UML/2.2/Superstructure/PDF

[3] Chaudhari H.C. and Kadam L.U. "Wireless Sensor Networks: Security, Attacks and Challenges", International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16.

[4] Pranav M. Pawar, Rasmus H. Nielsen, Neeli R. Prasad, Shingo Ohmoriand Ramjee Prasad, "Behavioural Modelling of WSN MAC Layer Security Attacks: A Sequential UML Approach", Center for TeleInFrastruktur, Aalborg University.

[5] TEODOR-GRIGORE LUPU, University "Politehnica" of Timisoara, Faculty of Automatics and Computers, Main Types of Attacks in Wireless Sensor Networks, Vasile Parvan 2, 300223, Timisoara, ROMANIA.

[6] Siebe Datema, :A Case Study of Wireless Sensor Network Attacks", Delft University of Technology, Delft University of Technology.