Simulation of Attacks for Security in Wireless Sensor Network

M. Sravan Kumar[1], D. Murali[2]

[1]*PG Student, Quba College of Engineering & Technology*

[2]*Assistant professor, Quba College of Engineering & Technology*

Abstract— The increasing complexity and low-power constraints of current Wireless Sensor Networks (WSN) require efficient methodologies for network simulation and embedded software performance analysis of nodes. In addition, security is also a very important feature that has to be addressed in most WSNs, since they may work with sensitive data and operate in hostile unattended environments.

In this paper, a methodology for security analysis of Wireless Sensor Networks is presented. The methodology allows designing attack-aware embedded software/firmware or attack countermeasures to provide security in WSNs. The proposed methodology includes attacker modeling and attack simulation with performance analysis (node's software execution time and power consumption estimation).

After an analysis of different WSN attack types, an attacker model is proposed. This model defines three different types of attackers that can emulate most WSN attacks. In addition, this paper presents a virtual platform that is able to model the node hardware, embedded software and basic wireless channel features. This virtual simulation analyzes the embedded software behavior and node power consumption while it takes into account the network deployment and topology.

Additionally, this simulator integrates the previously mentioned attacker model. Thus, the impact of attacks on power consumption and software behavior/execution-time can be analyzed. This provides developers with essential information about the effects that one or multiple attacks could have on the network, helping them to develop more secure WSN systems. This WSN attack simulator is an essential element of the attack-aware embedded software development methodology that is also introduced in this work.

I. STATE OF THE ART

Nodes in Wireless Sensor Networks are usually highly energy-constrained and are often expected to operate for long periods with limited energy reserves. For this reason, early performance estimation is an essential step in any embedded system design methodology. Early, fast and accurate simulations can provide information to the WSN developers that enable the modification of the SW algorithms or the network architecture in order to optimize the WSN design for the best use of the limited resources.

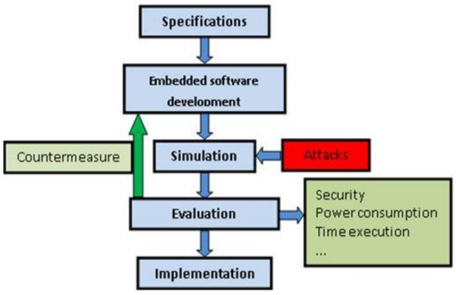

Figure 1. Firmware-aware attack design

This paper presents a methodology to design attack-aware embedded software/firmware or attack countermeasures. It makes use of a WSN simulator that includes attack simulation. The proposed methodology is presented in Figure 1. It includes a simulator that allows the evaluation of the network behavior under different conditions (different network topologies, attacks, software versions, etc.).

II. SECURE WSN DESIGN METHODOLOGY

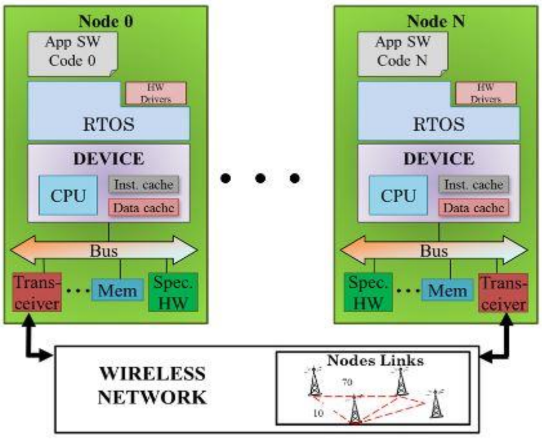

Figure 2. Scheme of Wireless Sensor Network virtual platform without attack model

The node model integrates processors, memories, RF-transceivers and sensors (see Figure 2). This allows the analysis of the functionality of each WSN node and the estimation its temporal and power consumption behaviors. These estimations are relevant features in order to evaluate the damage/impact of attacks. It also has a reliable network model than can be modified to evaluate any kind of network topology and deployment.

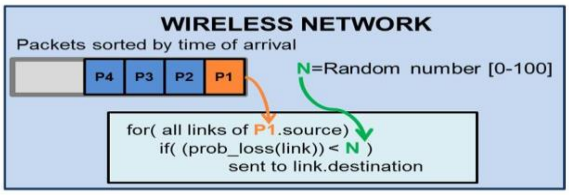
WIRELESS NETWORK
Packets sorted by time of arrival
P4
P3
P2
P1
N=Random number [0-100]
for(all links of P1.source)
if((prob_loss(link)) < N)
sent to link.destination

Figure 5. Normal network mode operation

When the simulation time matches the time of arrival of the packet, the wireless network pops the packet and generates a real random number between 0 and 100. If the packet-loss probability ("prob_loss (link)" in Figure 5) is lower than this random number, the network model transmits the packet to the destination node; otherwise, the packet is discarded. Figure 5 represents a scheme of this wireless network operation. Sensors 2016, 16, 1932 10 of 27 than this random number, the network model transmits the packet to the destination node; otherwise, the packet is discarded. Figure 5 represents a scheme of this wireless network.

III. MODELING OF WSN ATTACKS

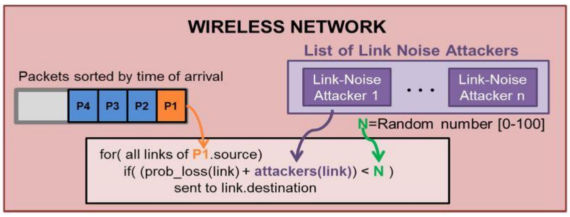
WIRELESS NETWORK
List of Link Noise Attackers
Packets sorted by time of arrival
Link-Noise Attacker 1
. . .
Link-Noise Attacker n
P4
P3
P2
P1
N=Random number [0-100]
for(all links of P1.source)
if((prob_loss(link) + attackers(link)) < N)
sent to link.destination

Figure 6. Network mode operation for Link Noise Attackers

Basically, this attacker modifies the packet-loss probability for certain packet types during predefined periods of time. The modification is presented in Figure 6. When a packet has to be transferred to the receiver node, the reception probability will include the original link probability and the additional noise produced by the attacker.

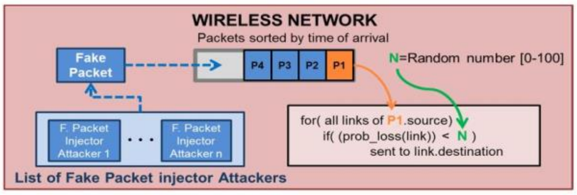
WIRELESS NETWORK
Packets sorted by time of arrival
Fake Packet
P4
P3
P2
P1
N=Random number [0-100]
F. Packet Injector Attacker 1
. . .
F. Packet Injector Attacker n
for(all links of P1.source)
if((prob_loss(link)) < N)
sent to link.destination
List of Fake Packet injector Attackers

Figure 7. Simulation with Fake Packet Injection attackers

Figure 7 shows how this attacker modifies the network model in Figure 5. The "Fake packet attacker" is responsible for generating the fake packets with the structure defined during the attacker configuration and introducing them directly into the transmission queue.

IV. EXPERIMENTAL RESULTS

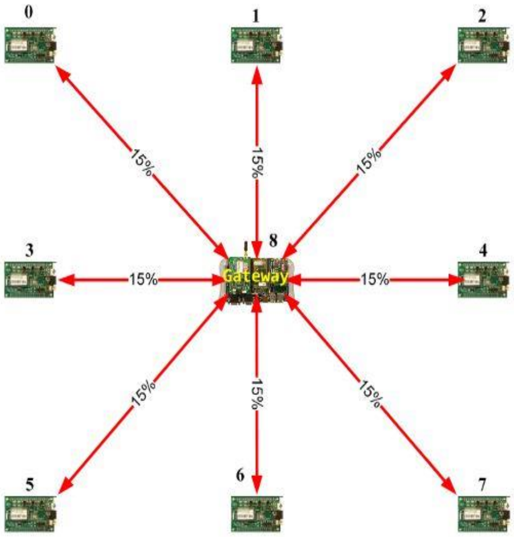

Figure 8: Meshed network example

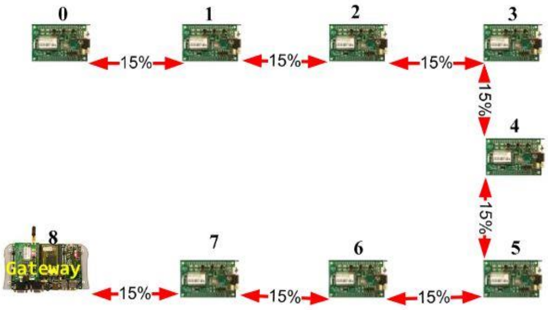

Figure 9. Linear network model example.

The first one is a meshed wireless network (Figure 8). Figure 9 shows the deployment of a linear wireless network and Figure 10 shows a circular wireless network. The percentages on the red lines represent the packet-loss probabilities of the wireless channel. If there is no red line between two nodes, it will be assumed that the packet-loss probability is 100% (no direct connection). In these examples, the packet loss probability is always the same (15%).

V. CONCLUSIONS

During the last years, there has been an increasing interest in WSN security. WSN attacks not only disrupt WSN behavior and allow access to restricted data but also increase the power consumption of the attacked nodes and reduce their battery life. The improvement in WSN security is a challenging problem because there is a wide variety of possible attack strategies that have to be analyzed. This paper proposes a methodology to increase WSN security that includes three main contributions.

Firstly, a methodology that allows the development of attack-aware embedded software. Secondly, an attack model that integrates some of the most important WSN attacks with only four categories. This model is used in the last contribution: a virtual platform that can simulate WSN under attacks. The attack model that has been presented in this paper is focused on active attacks, which mostly affect the network performance.

More precisely, it focuses on those attacks that try to disrupt, totally or partially, the communication flow among network nodes. Three types of attacker nodes have been identified: Link-noise, Fake-packet injection and Direct attack nodes. These attackers cover most of the vulnerabilities for WSN. The proposed virtual platform is able to model the node's HW, RTOS, embedded SW, and wireless network.

Additionally, the tool also models attacks over the WSN. All WSN attacks are modeled by using the attackers specified in the previously-defined attack model. Thus, the simulator can estimate the impact on behavior or power consumption that any node or the whole WSN network suffers under an attack.