Ingeniería e Investigación
ISSN: 0120-5609
ISSN: 2248-8723
Facultad de Ingeniería, Universidad Nacional de Colombia.

Gavric, Zeljko; Simic, Dejan

Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks

Ingeniería e Investigación, vol. 38, no. 1, 2018, January-April, pp. 130-138
Facultad de Ingeniería, Universidad Nacional de Colombia.

DOI: https://doi.org/10.15446/ing.investig.v38n1.65453

Available in: https://www.redalyc.org/articulo.oa?id=64358093016

DOI: http://dx.doi.org/10.15446/ing.investig.v38n1.65453

Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks

Visión general de los ataques de DOS en redes de sensores inalámbricos y resultados experimentales para la simulación de ataques de interferencia

Željko Gavrić[1], and Dejan Simić[2]

ABSTRACT

Wireless sensor networks are now used in various fields. The information transmitted in the wireless sensor networks is very sensitive, so the security issue is very important. DOS (denial of service) attacks are a fundamental threat to the functioning of wireless sensor networks. This paper describes some of the most common DOS attacks and potential methods of protection against them. The case study shows one of the most frequent attacks on wireless sensor networks – the interference attack. In the introduction of this paper authors assume that the attack interference can cause significant obstruction of wireless sensor networks. This assumption has been proved in the case study through simulation scenario and simulation results.

Keywords: Wireless Sensor Networks, Intrusion detection, Wireless communication, Communication system security, Radiofrequency interference.

RESUMEN

Las redes de sensores inalámbricos se utilizan ahora en varios campos. La información transmitida en las redes de sensores inalámbricos es muy delicada, por lo que el tema de la seguridad es muy importante. Los ataques de DOS (Denegación de servicio) son una amenaza fundamental para el funcionamiento de las redes de sensores inalámbricos. Este documento describe algunos de los ataques DOS más comunes y los posibles métodos de protección contra ellos. El estudio de caso muestra uno de los ataques más frecuentes a las redes de sensores inalámbricos: el ataque de interferencia. En la introducción de este artículo, los autores suponen que la interferencia de ataque puede causar una obstrucción significativa de las redes de sensores inalámbricos. Esta suposición se ha demostrado en el estudio de caso a través de escenarios de simulación y los resultados de estas simulaciones.

Palabras clave: Redes de sensores inalámbricos, detección de intrusión, comunicación inalámbrica, seguridad del sistema de comunicación, interferencia de radiofrecuencia.

Received: June 6th 2017
Accepted: November 20th 2017

Introduction

Wireless sensor networks – WSN are created with the purpose of collecting and analyzing data in real time. They are mainly intended to work with small amounts of data. WSN are most commonly used for environmental observations, tracking natural catastrophes, control of business processes, smart environments (smart houses, smart buildings, smart parking), traffic tracking, medical applications, etc.

WSNs consist of individual sensor nodes (SNod). These sensor nodes gather environmental data, collaborate with each other and send the measured data via wireless communications to the sink (Fan, 2016). The sink takes data from sensor nodes, analyses and synthesizes them and serves the purpose of interface for the outside world. The sink is usually connected to the end user through the use of existing network infrastructures such as internet or GSM networks. Within one sensor network there are usually hundreds, even thousands of sensor nodes, which communicate with the sink. Typical sensor node consists of (Dargie *et al*., 2010):

- Sensor, which is in charge of converting the observable physical size to electronic
- Processor, which is in charge of receiving, sending and processing sensor data

[1] Engineer of Informatics, M.Sc., Faculty of Information Technology, Slobomir P University, Bosnia and Herzegovina. Affiliation: Teaching assistant, Faculty of Information Technology, Slobomir P University, Bosnia and Herzegovina. E-mail: zeljko.gavric@spu.ba

[2] Electrical Engeener, Ph.D., Faculty of Electrical Engineering, University of Belgrade, Serbia. Affiliation: Full professor, Faculty of Organisational Sciences, University of Belgrade, Serbia. E-mail: dsimic@fon.bg.ac.rs

How to cite: Gavrić, Ž., Simić, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ingeniería e Investigación,* 38(1), 130-138.
DOI: 10.15446/ ing.investig.v38n1.65453

- Communication subsystem, which is in charge of sending and receiving data
- Power supply subsystem, which is in charge of securing autonomy of sensor node.

Apart from the components listed above, sensor nodes can have additional components such as a GPS module which is used for determining the location of the sensor node. Sensor nodes can also have actuators with which they influence the observed process. In case additional modules which require a vast amount of energy are used, it is very difficult to sustain the energetic stability of a sensor node. Sensor nodes have limited resources, such as the battery power supply, weak processing ability and similarly. It is possible to prolong battery lifetime in scarce environments of energy by using several different energy efficiency techniques. There are approaches based on power saving techniques such as data compression (Distribution Compressive), improvements to routing algorithms and the method of hibernating of the sensor node (Oliveira, 2015).

Most wireless sensor nodes are placed on uncontrolled terrain, where there are various safety hazards. It is important to determine those hazards and take necessary precautions to secure proper network functioning.

This paper consists of a theoretical and an experimental part. Theoretical part has two sections. Section 2 describes the basic principles of communication in WSN. It shows the protocol stack and explains the layers of the protocol stack. Section 3 describes DOS attacks and potential solutions for detect and prevent of some attacks. The attacks are sorted by protocol stack layers. Distributed DOS attacks are described like special category of DOS attacks. The experimental part shows a realization of an attack, where the attacker interferes with proper functioning of wireless network. This attack is one of the most commonly used attacks and can cause a complete shutdown of a WSN.

This paper begins with assumption that interference can cause serious obstruction of a WSN, which means it can lead to loss of packets being transferred within the WSN. Besides that, there is an assumption that interference depends on the distance between the attacker and the network node, therefore, in the experimental part the authors consider how the distance between the sink and the attacker affects the outcome of the attack.

Related works

Many papers describe the taxonomies of DOS attacks. Most of those papers show attacks clasified by protocol stack layers (Raymond *et al*., 2008; Wood 2002). Some of papers show attacks classified on pasive and active (Shahzad *et al*., 2017).

Radio interference attack is described in Hamieh *et al*. (2009), Nancy *et al*. (2014) and Hamza *et al*. (2016).

WSN performance under some attacks is described in Rupayan *et al*. (2016). This paper shows how does the interference reduces throuput of WSN.

Communication in wireless sensor networks

Sensor nodes are scattered on the sensor array. All sensor nodes send data to sink. In order for sensor nodes to send the data properly to the sink and vice versa, it is necessary to obey the rules of communication – protocols. Figure 1 shows protocol stack which is used with WSN.

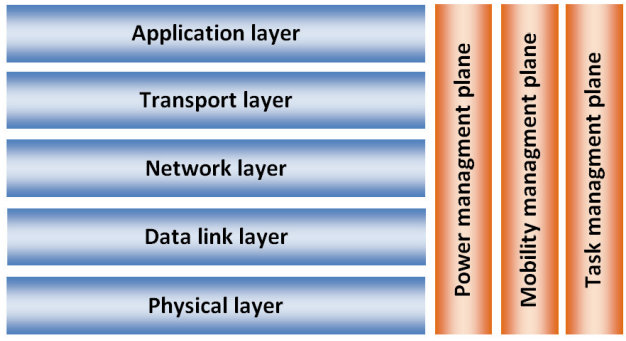

Figure 1. Protocol stack for WSN.
Source: Pomalaza (2004)

The picture shows that all used protocols are distributed in 5 layers: application, transport, network, data connection layer and physical layer that is consistent to TCP/IP layered model.

Application layer's function is to separate hardware and software from end user. Because of that it is possible to create and use a vast amount of different applications. Different protocols are used depending on the task the sensors are supposed to do.

Transport layer must secure the data transfer from sensor nodes to the sink. End to end reliability is not implemented between individual sensors and the sink, but between the event and the sink. Event consists of group of sensor nodes which can detect observed occurrence. Simultaneously, the sink usually sends data to a specific sensor node.

Network layer is responsible for data routing in WSN. Except routing, transport layer must provide energy efficiency and the data aggregation. Routing is performed using any of the techniques of routing, such as flooding or gossiping (Fan, 2016).

Data link layer is responsible for multiplexing data stream, detecting data frames, medium access and error detection (Dargie, 2010).

Physical layer is responsible for choosing frequency, generating frequency carrier, signal detection, modulation of data. Most commonly frequencies from ISM (industrial, scientific, and medical) range are used. Generating

frequency carrier and signal detection depend on hardware limitations, and the goal is to be simple, save energy, and achieve the lowest price of the final product. Most commonly binary and M-ary modulation schemes are used. Binary modulation schemes are cheap because of their simple implementation, and thus they are characterized by better power efficiency (Pomalaza, 2004).

Apart from layers which are consistent with TCP/IP model, there are also planes, like the plane for power control, the plane for movement control and the plane for task control. Planes overlook power consumption, movement and distribution of tasks between sensors. They enable reduction of total power consumption and help with coordination in the data collection process.

Data connection layer and physical layer are defined with 802.15.4 standard. This standard defines personal wireless small speed networks. It represents the basis for technologies such as ZigBee, ISA100.11a, WirelessHART, MiWi, SNAP and Thread (Callaway *et al*., 2002).

DOS attacks

Considering that radio media is used to transfer data within WSN, the very process of sending is subject to various safety risks and threats. Sensor nodes have limited resources. Therefore, it is often not possible to protect them with sophisticated safety protocols and techniques. Safety protocols and mechanisms within WSNs are developed in such a way that they secure the network on a satisfactory level using as little resources as possible. In contrast to sensor nodes, attacker can use equipment which has much larger resources and capabilities, such as stronger antennas for signal emission, constant power supply, strong processor and memory capacity. This is part of the reason why number of attacks on WSNs is increasing.

Attacks on WSNs are aimed to jeopardize network functioning, in order to abuse data which is being transferred within the network, to spy on or interfere with network. Attacks can be classified according to the layer of protocol stack that they are attacking.

One of the most common attacks on WSNs, and that goes through all layers of protocol stack, is DOS attack. The main aim of this attack is to disable proper functioning of the network. Attacker or attackers, using various types of attacks, prevent the legitimate network nodes from using the network resources. If the network is being attacked by multiple attackers, that situation is called a distributed attack. This kind of attack can cause significantly more problems in network functioning than attacks on a single node. Attacker can be an outside node, which is not a part of WSN, or it can be one of the legitimate nodes that's been compromised by the attacker. Some of the indicators of DOS attack are (Buch *et al*., 2010):

- Decrease in network performance;
- Parts of the network are not responding;
- Increase of spam messages;
- Delay or loss of packets and their confirmations.

In Table I the most common DOS attacks are shown, classified according to protocol stack layers.

Table 1. Dos attacks

Layer	Attacks
Physical layer	Jamming Interference Node tampering and destruction
Link layer	Collision Exhaustion Unfairness
Network layer	Sybil Selective forwarding Sinkhole Hello flooding Wormhole
Transport layer	Flooding Desynchronization
Application layer	Overwhelming sensors (sensor overload) Path based attack

Source: Authors

DOS attacks depending on their level of destructiveness can be classified in following groups (Buch *et al*., 2010):

- Attacks which waste resources, such as memory, processing time, bandwidth and similar
- Attacks which delete or change rooting information
- Attacks which interrupt information about network status, such as interrupting TCP session
- Attacks which interfere the communication between legitimate nodes

DOS attacks classification by protocol stack layers

This chapter explains different types of DOS attacks classified by protocol stack layers.

DOS attacks at physical layer

Jamming is one of the most common DOS attacks on WSNs. Attacks are defined as constant interference, random, deceptive and reactive functions. In case of constant jamming, data is emitted by the attacker in regular time intervals. Flooding attack happens when the attacker acts like a legitimate node within the network and continuously sends data. Also when the attacker notices data transfer within the network he then emits jam signal. Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters

a "sleeping" mode. It will resume jamming after sleeping for some time (Xu *et al*., 2006). Another kind of jammer is a deceptive jammer. It sends a constant stream of bytes into the network to make it look like legitimate traffic (Raymond *et al*., 2008). An alternative approach to jamming wireless communication is to employ a reactive strategy. A reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel (Xu at al., 2006).

Counter measures: Spread spectrum technique helps in avoiding these kinds of attacks (Raymond *et al*., 2008). Aside from spread spectrum technique, nodes must have their own strategy to confront jamming attacks. Such as putting node into sleep mode during the duration of jam signal, in order to preserve power efficiency, also periodically waking up nodes in order to check if the jamming signal is still active (Ghildiyal *et al*., 2014). In the paper (Nancy *et al*., 2014), the new approach for detection and protection from jamming attacks, is described. This approach uses two modules which determine the level of interference in WSN. First module protects the network from internal nodes that are marked as nodes which previously emitted large amounts of jamming signal. Second module detects new potential attacker nodes. Results shown in the paper reveal that this approach offers high level of attacker detection.

Interference occurs when the attacker generates large amounts of network traffic in the form of radio waves, periodically or constantly in order to interfere with network functioning.

Counter measures: Symmetrical key algorithm with delayed revelation of keys during the pause is used in order to solve this problem (Raymond *et al*., 2008). In the work presented by Danyang *et al*. (2013), the use the mechanism with adaptive filtering on bases of predetermined threshold of interference in order to gain more efficient frequency range is suggested. This mechanism contributes to a decrease of interference and to more efficient use of resources within WSN.

Node destruction occurs when attacker gains physical access to the node and disables its functioning or gains access to its memory with the aim to change the information which secures proper functioning. Defective node causes interference in communication.

Counter measures: The way of protection from physical access to the node is setting up a physical package to protect it or placing the node on hardly accessible location (Raymond *et al*., 2008).

DOS attacks at data link layer

Collision occurs when two nodes try to send packets at the same time on the same frequency. Loss of packet or sum control error appears in the transmitter that sends messages. The malicious node tries to send data at the same time as legitimate nodes in order to intercept the arrival of the packet from the legitimate node to the receiver.

Counter measures: To overcome this problem ECC (error correction code) must be used. Most codes correct lesser collisions, but they require additional processor capacity and communication resources. The main problem is that the attacker is capable of generating more errors than can be corrected (Raymond *et al*., 2008). In the paper (Dbibih *et al*., 2016) a new algorithm for limiting access to medium CAMAC, is shown. The function of this algorithm is to prioritize every message in order to minimize the number of collisions.

Exhaustion occurs in the case of constant collisions, which leads to a complete congestion of the channel. Usually the attacker sends large number of RTS (requests to send).

Counter measures: One of the solutions to this is for MAC (Medium Access Control) to reject enormous number of requests from a specific node (Amara *et al*., 2013). Other solution for this kind of attack is to use time multiplexing, i. e. to set a time limit for the access medium and in that way to reject attacker's excessive number of requests (Ghildiyal *et al*., 2014).

Unfairness occurs with illegal use of connection layer mechanism that obstructs regular activities. Unfairness occurs with collision or constant access to the channel.

Counter measures: In order to minimize unfairness it is necessary to use small rams by all sensor nodes. When small rams are used all nodes deny access to the channel for short periods of time (Saxena, 2007).

DOS attacks at network layer

Sybil attack occurs when the malicious node presents multiple identities to other nodes in the network. A node can appear in multiple locations or multiple times in a single network. It can be very complicated for the attacker to convey this type of attack in the network in which every pair of neighboring nodes uses a unique key for initialization or frequency hopping in expanded range. With Sybil attacks when routing protocols are attacked, the malicious node takes identity of multiple nodes which leads to conveying multiple routs through it.

Counter measures: Defense against Sybil attacks is achieved through identity check and through use of ID based key and location based key (Shahzad *et al*., 2017). In the paper (Yong *et al*., 2006), the way to detect Sybil attack using inquiries is described. This is achieved through sending inquiries to the nodes in the cluster by the master node in the cluster.

Selective forwarding is an attack which occurs when the malicious node rejects some of the received packets, and forwards others. The attacker can reject packets according

to certain criteria. Therefore it can forward all the packets received from a certain node and reject all the packets from another node. Specific case of this type of attack is rejection of all packets, but in this case the neighboring nodes easily detect the malicious node, and start using alternative routes.

Counter measures: Solution to this kind of attack is using multiple routes (Hossain *et al*., 2015). In the paper (Mathur *et al*., 2015), modified protocol for safe routing is described. This protocol has the ability to detect attacks on routing, such as selective forwarding.

Sinkhole is an attack which occurs when the malicious node is positioned in such way that all data traffic of a certain area is routed through it, and its role is to reject all received packets. The malicious node is identified by surrounding nodes as the most efficient node to send data through. The node achieves this by reducing the number of jumps to the sink using a strong transmitter. The longer malicious node operates within the network, the more rapidly the number of nodes that send data through it increases. A sinkhole attack can be achieved using an artifical beneficial route. In this type of attack the intruder has greater computational and communication power than other nodes and manages to create a high quality single hop connection with the base station. It then emits its high quality routing message to its neighbors. After this, all the neighbors divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched (Chaudhry *et al*., 2013).

Counter measures: One of the solutions for this type of attacks is the use of geographic routing protocol (Yong *et al*., 2006). In the paper (Wazid *et al*., 2013), algorithm which detects and prevents this type of attack is described.

Hello flooding occurs when attacker sends a broadcast hello message using equipment which has strong emission power. The message is received by a large number of nodes that detect surrounding nodes as the attacker, even though the real attacker is usually distanced from the node and actually is out of their range. Legitimate nodes send messages towards the attacker, and in case the attacker receives these messages he rejects or abuses them in other ways. In case messages are not delivered to the attacker node, their content is lost. Namely, large number of protocols requires broadcast sending of 'hello' message by every single node (Singh *et al*., 2010). Every node presents the message to his neighbors, so they can communicate with it. For this type of attack, the attacker usually uses a laptop of a much stronger configuration then the sensor nodes.

Counter measures: Solution to this kind of attack is the use of authentication by the third node (Yong *et al*., 2006) or geographic routing protocol (Raymond *et al*., 2008). In the paper (Maheswari *et al*., 2016) new safety routing scheme RAAED is presented. This scheme is based on enhanced bidirectional verification scheme. The attacker can be identified by checking the average signal strength of the nodes within network, therefore the node with greater signal strength then the surrounding nodes is the potential attacker (Maleh *et al*., 2016).

Wormhole attack occurs when the attacker tunnels data traffic between one part of the network and the other, using direct slow speed connection. For this attack usually two malicious nodes are used, one of which is near the sink. One node is presented to other surrounding nodes as the best node for forwarding data to sink. The forwarding usually seems executable in one jump, using a tunnel between the two malicious nodes.

Counter measures: Possible minimization of this kind of attack can be achieved through geographic routing protocol; same as for Sinkhole attack (Hossain *et al*., 2015). In the paper (Goyal *et al*., 2015) defenses against wormhole attacks are sorted into following categories: location and temporal based defense approach (it is based on time synchronization and distribution of secret keys), defense approach based on connection and surrounding nodes (it is based on jump count and listing of neighboring nodes), and approach based on topology (it is based on adding extra elements that deal with network monitoring).

DOS attacks at transport layer

Flooding occurs when the attacker sends large number of requests for establishing connection, therefore depleting resources of legitimate nodes. Namely, transport layer protocols are sustaining end to end connection, so sending a request for establishing the connection is required every time we want to establish the connection.

Counter measures: This kind of attack is solved by limiting the number of connections that a single node can establish, but in this case it is possible for a legitimate node to fail to connect (Saxena, 2007). Solution offered in Amara *et al*. (2013) requires that the node which needs to establish the connection with another node must first solve a puzzle. For the attacker this requires additional resources, and prevents the establishment of a large number of connections in short period of time.

Desynchronization refers to disconnection of established connection. The malicious node requires constant sending of requests for establishing connection from one or both nodes between which the connection is established. This way the established connection desynchronizes, and besides that, additional power is wasted on responding to the malicious node.

Counter measures: Solution for this kind of attack is to authenticate all packets being exchanged between sensor nodes, including all fields of packet header (Benbrahim, 2011).

DOS attacks at application layer

Sensor overload occurs when the attacker tries to overload the node by stimulating sensors, which causes forwarding of large amount of data traffic towards the sink. This attack overloads the bandwidth and wastes node's power.

Counter measures: This kind of attack is preventable by setting sensors' sensitivity, as well by limiting the speed of data sending from the nodes (Raymond *et al*., 2008). Limiting bandwidth and efficient aggregation can successfully reduce effectiveness of this attack.

Path based attack occurs when the attacker injects replayed packets to flood the end to end communication between two nodes. Every node in the path towards the base station forwards the packet, and if large number of fake packets are sent all of these become busy. So, this attack consumes network bandwidth and energy of the nodes (Deng *et al*., 2005).

Counter measures: The solution is to choose a good authentication method or anti replay protection (Isha *et al*., 2013).

Distributed DOS attacks

Distributed DOS attacks – DDOS (distributed denial of service) represents special group of attacks during which multiple nodes in cooperation attack the WSN. In this situation the attacked node is being flooded by hundreds or even thousands of different nodes (Wesam *et al*., 2014).

DDOS attack consists of four elements (Sonar *et al*., 2014):

- Real attacker
- Compromised nodes which are running a special program (handler), and have the ability to control multiple agents
- Agent nodes, which execute special program that is responsible for generating streams of data towards victim (the attacked node). These nodes are usually outside of victim's network
- Victim

The flow of DDOS attack is shown in Figure 2:

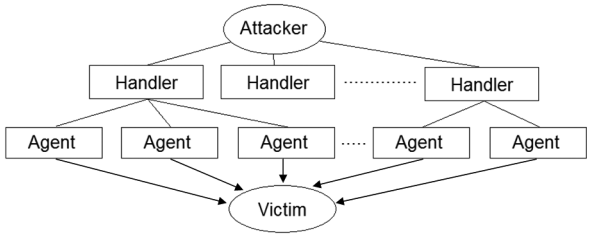

Figure 2. The flow of DDOS attack
Source: Malik *et al*. (2015)

In the paper (Mopari *et al*., 2008) DDOS attacks are classified into volume based attacks, protocol based attacks and application layer based attacks. In the following table detailed classification of DDOS attacks is shown.

Table 2. DDOS attacks

Category of DDOS attack	Attacks
Volume based attacks	ICMP flooding UDP flooding Spoofed-packet flooding
Protocol based attacks	SYN flooding Fragmented packets Ping of death Smurf
Application layer based attacks	Zero-day Slowloris

Source: Authors

There are many ways to prevent and detect DDOS attacks. Some of them are shown in following text.

In Mopari *et al*. (2008) a mechanism which is focused on detection and rejection of false packets is shown. Packet authenticity is checked by the estimated number of jumps required for packet to reach its destination. Table of jump numbers is created with purpose of finding and memorizing the number of packet hops. This table is used for discovering false packets which are discarded in filtering phase.

DAT (Liu *et al*., 2011) is model of defense which analyzes the behavior of nodes in order to determent whether the node is real or false.

Depending on the activities conducted by the user, system evaluates whether the node is valid, and it eventually takes steps towards disconnecting it from network.

In Choi *et al*. 2010) integrated infrastructure for defense from DDOS attacks is presented. Firstly, attack is divided into three phases, than requirements for defense are shown for each phase. When all requirements are met, integrated infrastructure is created IDDI.

Sahu *et al*. (2014) present the system for network data filtering whose aim is to prevent DDOS. Network filter tracks data traffic from nodes, and if it detects that a node emits large quantity of data in short time intervals, it determines that the node is the attacker and discards its packets that are being sent to sink.

Modern systems for attack detection IDS (Intrusion Detection System) collect information from network, save the information and based on detailed data analysis detect the attacker in the network (Shanthi *et al*., 2016). These systems contain procedures and mechanisms for detection, prevention and reaction in case of attack.

Case study

In the practical part of this paper, the authors describe one way of provoking a DOS attack. As it was mentioned previously, DOS attacks aim to disable proper network functioning. This is one of very common attacks on WSN.

The authors describe and implement a scenario of this type of attack in the following text by adding an attacker node to WSN. The attacker emits large quantity of data traffic with the aim to disable other nodes in the network from successfully sending their data to sink. Simulator Omnet++ (https://omnetpp.org) and Castalia module (https://forge.nicta.com.au) for simulation of WSNs are used to simulate this scenario.

WSN which is used for the simulation consists of 5 legitimate sensor nodes, of which one represents sink. The sink is represented by node 0, while remaining 4 nodes try to send data to the sink. If there is no attacker, the sink receives data from 4 legitimate nodes. If there is an atacker in the WSN area, the sink doesn't receive all the packets sent from legitimate nodes. The authors want to find out how many packets the sink would receive in case the attacker moves to a different distance from the sink. For this purpose the authors used throughput test aplication, where all legitimate nodes send packets to the sink. This application shows all received packets from nodes. The throughput test application is described in detail in Boulis (2011).

In Figure 3 simulation scenario is shown.

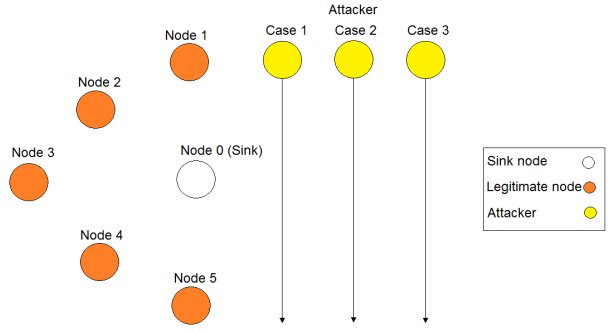

Figure 3. The flow of DDOS attack.
Source: Authors

Legitimate nodes in the network are static and they are located on proper distance from one another in order to avoid interference. Attacker node is mobile node, which means it moves in preset manner. In specified periods of time attacker node will cause interference which will disable sink from receiving data from legitimate nodes.

In simulation scenario attacker nodes is moving forward in a straight line on predefined distance from sink. Few sub scenarios are implemented which have different minimum distance from the line in which attacker node moves towards sink, and in this process the number of received packets by the sink is tracked.

After testing different sub scenarios different results were acquired depending on the distance of the attacker node. In the following table summary results of testing are shown.

Table 3. Testing results

	Without attacker	With attacker		
		Distance from sink 10 m	Distance from sink 20 m	Distance from sink 30 m
Number of received packets	187	25	73	124
Number of non received packets	0	162	114	63

Source: Authors

As it is seen in the test results, interference increases when attacker node gets closer to the sink. Number of packets that are being received significantly drops when attacker node approaches the sink. When attacker is at 10m, 20m and 30m distance from the sink, it receives 13,36% packets, 39,04% packets and 661,31% packets respectively. In Figure 4 diagram of simulated scenario is shown. Number of sent packets and received packets by the sink depending on the distance of attacker node from the sink is shown on diagram.

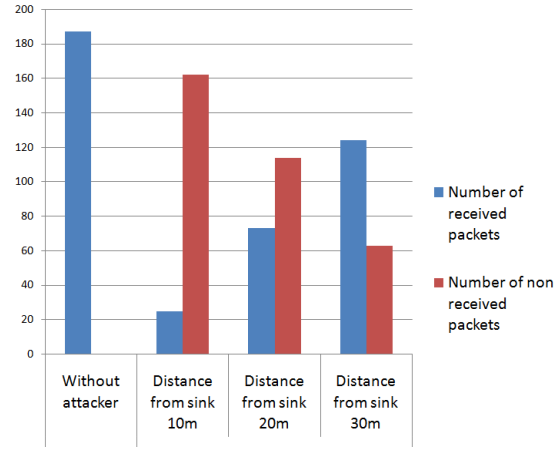

Figure 4. Diagram of testing results.
Source: Authors

With detailed analysis of received packets it is clear that the sink received the least packets from nodes 1 and 5 which were the closest to the route on which the attacker node is moving. That means that the attacker jamming route beetwen legitimate nodes and the sink and the distance of the attacker are significant factors for the achievement of a physical DOS attack.

From listed examples it can be concluded that interference attack is a very serious attack that can disturb proper functioning of WSN. This kind of attack is fairly easy to implement, which brings up the importance of using adequate defense against it.

Conclusion

Research area of WSNs is very active and new technologies are being developed constantly. Given the prevalence of WSNs various security issues may arise. One of the big issues is that nodes of WSN are often placed on various locations, which are usually difficult to secure from physical access. Safety omissions not only can jeopardize proper functioning of WSN, but they can also lead to spreading of false information within the network. This may cause for user to receive wrong data, and to make wrong decision based on them, which could potentially lead to catastrophic consequences on the observed environment.

This paper included basic threats which are threatening WSN on daily basis. The main part of the paper describes DOS attacks on WSN and solutions suggested by literature for detecting and solving particular attacks. This type of attack leads to a complete or partial shutdown of WSN, and therefore it is not strange that large amount of research is conducted daily in order to protect WSN from different kinds of DOS attacks. DOS attacks can be divided in multiple categories. In this paper the authors use a categorization of attacks according to protocol stack layers. The most threatening attacks are DOS attacks on physical layer, DOS attacks on connection layer, DOS attacks on network layer, DOS attacks at transport layer and DOS attacks at application layer.

In the case study described in this paper influence of DOS interference attacks is shown, they emit large quantities of data in the form of radio waves that disable information flow from legitimate nodes to sink. Few situations have been tested in Omnet++ simulator by using Castalia simulation model for simulating WSNs. The results generated by the simulation were shown.

The main assumption of the authors was that interference attacks disrupt WSN functioning. This assumption has been proven in the experimental part of the paper. Based on generated test results it can be determined that significant packet losses occur during the attack, i. e. in the used scenario information flow from sensor nodes to the sink has been mostly disabled. Case study shows that distance of the attacker is a significant factor when an interference attack occurs.

References

Fan, C. S. (2016). HIGH: A Hexagon-based Intelligent Grouping Approach in Wireless Sensor Networks. Advances in Electrical and Computer Engineering, vol.16, no.1. 41-46, 2016. DOI: 10.4316/AECE.2016.01006

Dargie W., & Poellabauer, C. (2010). Fundamentals of wireless sensor networks: theory and practice. John Wiley & Sons.

Oliveira, F., Semente, R., Fernandes J., Júnior, S., Melo, T., & Salazar, A. (2015). EEWES: An energy-efficient wireless sensor network embedded system to be applied on industrial environments. Ingeniería e Investigación, 35(2), 67-73. DOI: http://dx.doi.org/10.15446/ing.investig.v35n2.45289

Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. computer, 35(10), 54-62.

Das, R., Bal, S., Das, S., Sarkar, M. K., Majumder, D., Chakraborty, A., & Majumder, K. (2016, October). Performance analysis of various attacks under AODV in WSN & MANET using OPNET 14.5. In Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual (pp. 1-9). IEEE.

Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. IEEE Network, 20(3), 41-47.

Pomalaza, C. (2004). Wireless sensor network. University of Oulu, Finland.

Callaway, E., Gorday, P., Hester, L., Gutierrez, J. A., Naeve, M., Heile, B., & Bahl, V. (2002). Home networking with IEEE 802.15. 4: a developing standard for low-rate wireless personal area networks. IEEE Communications magazine, 40(8), 70-77.

Hossain, M., Muslima, U., & Islam, H. (2015). Security Analysis of Wireless Sensor Network. Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2 – Issue 1, pp. 393-403, 2015. DOI: 10.1155/2014/303501

Buch, D., & Jinwala, D. C. (2010). Denial of Service Attacks in Wireless Sensor Networks. International conference on current trends in technology, Nuicone.

Shahzad, F., Pasha, M., & Ahmad A. (2017). A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. International Journal of Computer Science and Information Security, Vol. 14, No. 12. arXiv preprint arXiv:1702.07136

Isha ,Arun, M., & GauravR. (2013). DOS Attacks on TCP/IP Layers in WSN. International Journal of Computer Networks and Communications Security VOL. 1, NO. 2, 40–45.

Raymond, D.R., & Midkiff, S.F. (2008). Denial of Service in Wireless Sensor Network: Attacks and Defenses. IEEE Pervasive Computing, Vol. 7, Issue 1, pp.74-81. DOI: 10.1109/MPRV.2008.6

Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. IJRET: International Journal of Research in Engineering and Technology, Vol. 3, eISSN: 2319-1163, pp.140-143.

Nancy, J. T., VijayaKumar, K. P., & Kumar, P. G. (2014). Detection of jammer in Wireless Sensor Network. International Conference on Communications and Signal Processing (ICCSP), IEEE, 1435-1439. DOI: 10.1109/ICCSP.2014.6950086

Danyang, Q., Lin, M., Erfu, W., Hongbin, M., & Qun, D. (2013). An interference suppression mechanism for WSN. International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS), IEEE, 28-33. DOI: 10.1109/SNS-PCS.2013.6553829

Dbibih, I., Iala, I., Aboutajdine, D., & Zytoune, O. (2016). Collision avoidance and service differentiation at the MAC

layer of WSN designed for multi-purpose applications. Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference, IEEE, 277-282. DOI: 10.1109/CloudTech.2016.7847710

Amara, S. O., Beghdad, R., & Oussalah, M. (2013). Securing Wireless Sensor Networks: A Survey. EDPACS, 47(2), 6-29. DOI: 10.1080/07366981.2013.754207

Saxena, M. (2007). Security In Wireless Sensor Networks - A Layer Based Classification. CERIAS Tech Report.

Yong, W., Garhan, A., & Byrav, R. (2006). A Survey Of Security Issues In Wireless Sensor Networks. IEEE Communications Surveys & Tutorials, Volume 8. DOI: 10.1109/COMST.2006.315852

Mathur, A., & Newe, T. (2015). Medical WSN: Defense for selective forwarding attack. Sensing Technology (ICST), 2015 9th International Conference, IEEE, 54-58. DOI: 10.1109/ICSensT.2015.7438364

Wazid, M., Katal, A., Sachan, R. S., Goudar, R. H., & Singh, D. P. (2013). Detection and prevention mechanism for blackhole attack in wireless sensor network. Communications and Signal Processing (ICCSP), 2013 International Conference IEEE, 576-581. DOI: 10.1109/iccsp.2013.6577120

Chaudhry, J. A., Tariq, U., Amin, M. A., & Rittenhouse, R. G. (2013). Dealing with sinkhole attacks in wireless sensor networks. Advanced Science and Technology Letters, 29(2), 7-12.

Maheswari, S. U., Usha, N. S., Anita, E. M., & Devi, K. R. (2016). A novel robust routing protocol RAEED to avoid DoS attacks in WSN. Information Communication and Embedded Systems (ICICES), 2016 International Conference, IEEE, 1-5. DOI: 10.1109/ICICES.2016.7518942

Maleh, Y., & Ezzati, A. (2014). A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks. International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 6. arXiv:1401.1982 [cs.CR]

Goyal, S., Bhatia, T., & Verma, A. K. (2015). Wormhole and Sybil attack in WSN: A review. Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference, IEEE, 1463-1468.

Singh, V. P., Jain, S., & Singhai, J. (2010). Hello flood attack and its countermeasures in wireless sensor networks. IJCSI International Journal of Computer Science Issues,7(11), 23-27.

Benbrahim, S. E. (2011). Defense against traffic analysis attack in wireless sensor networks. PhD Thesis, University of Montreal, Canada.

Deng, J., Han, R., & Mishra, S. (2005). Defending against path-based DoS attacks in wireless sensor networks. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks (89-96). ACM.

Wesam B., & Mehdi, E. M. (2014). Review Clustering Mechanisms of Distributed Denial of Service Attacks. Journal of Computer Science 10, pp. 2037-2046. DOI: 10.3844/jcssp.2014.2037.2046

Sonar, K., & Upadhyay, H. (2014). A Survey: DDOS Attack on Internet of Things. International Journal of Engineering Research and Development, 10, 58-63.

Malik, M., & Singh, Y. (2015). A Review: DoS and DDoS Attacks. International Journal of Computer Science and Mobile Computing, Vol. 4 Issue 6, 260-265.

Mopari, I. B., Pukale, S. G., & Dhore, M. L. (2008). Detection and defense against DDoS attack with IP spoofing. Computing, Communication and Networking, ICCCn 2008, International Conference, IEEE, 1-5. DOI: 10.1109/ICCCNET.2008.4787693

Liu, H. I., & Chang, K. C. (2011). Defending systems against tilt DDoS attacks. Telecommunication Systems, Services, and Applications (TSSA), 2011 6th International Conference, IEEE, 22-27. DOI: 10.1109/TSSA.2011.6095400

Choi, Y. S., Oh, J. T., Jang, J. S., & Ryou, J. C. (2010). Integrated DDoS attack defense infrastructure for effective attack prevention. Information Technology Convergence and Services (ITCS), 2010 2nd International Conference, IEEE, 1-6. DOI: 10.1109/ITCS.2010.5581263

Sahu, S. S., Priyadarshini, P., & Bilgaiyan, S. (2014). Curbing Distributed Denial of Service attack by traffic filtering in Wireless Sensor Network. Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference, IEEE, 1-6. DOI: 10.1109/ICCCNT.2014.6963043

Shanthi, S., & Rajan, E. G. (2016). Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. Next Generation Computing Technologies (NGCT), 2016 2nd International Conference, IEEE, 426-431. DOI: 10.1109/NGCT.2016.7877454

Hamieh, A., Ben-Othman, J., & Mokdad, L. (2009). Detection of radio interference attacks in VANET. Global Telecommunications Conference, Globecom 2009, IEEE, 1-5. DOI: 10.1109/GLOCOM.2009.5425381

Hamza, T., Kaddoum, G., Meddeb, A., & Matar, G. (2016). A Survey on Intelligent MAC Layer Jamming Attacks and Countermeasures in WSNs. Vehicular Technology Conference (VTC-Fall), IEEE 84th, IEEE, 1-5. DOI: 10.1109/VTCFall.2016.7880885

Boulis, A. (2011). Castalia - A simulator for Wireless Sensor Networks and Body Area Networks. NICTA: National ICT Australia.