Analysis of the WSN MAC Protocols under Jamming DoS Attack

Boris Mihajlov [1] and Mitko Bogdanoski [2]
(Corresponding author: Mitko Bogdanoski)

European University[1]
Blvd "Kliment Ohridski" 68, 1000, Skopje, R. Macedonia
Military Academy "General Mihailo Apostolski, Goce Delcev University, an associated member"[2]
Vasko Karangelevski bb, 1000, Skopje, R. Macednia
(Email: mitko.bogdanoski@ugd.edu.mk)

(Received June 30, 2013; revised and accepted Oct. 12, 2013)

Abstract

Wireless Sensor Network (WSN) is a wireless network consisting of small nodes with sensing, computation, and wireless communications capabilities. The design of wireless sensor networks depends of many factors, such as transmission errors, network topology and power consumption. Many routing protocols, protocols for data transmission, are specifically designed for wireless sensor networks where energy consumption is essential. This paper provides a brief description of the IEEE 802.15.4/ZigBee standard, also surveys the known attacks on wireless sensor networks. WSNs are particularly vulnerable to several key types of attacks. These attacks can be performed in several different ways. One of the commonly used methods is a denial of service (DoS), but there are also other types of attacks from which we should be aware as a traffic analysis, privacy violation, physical attacks etc. Three MAC protocols, such as IEEE 802.15.4 MAC, T-MAC, and S-MAC are proposed to analyse the performance of the WSN under DoS attack using OMNeT++ simulator. Different application scenarios have been evaluated. Performance parameters such as throughput, network delay, energy consumption in the coordinator, and network load are the main considered factors in our study.

Keywords: Dos, IEEE 802.15.4, jamming, OMNeT++, wireless sensor network, ZigBee

1 Introduction

In 1999 it was named as one of "21 ideas for the 21st Century" [1], and in 2003 was presented as one of "10 new technologies that will change the world" [7]. This revolutionary technology is known as WSNs. WSN is an area of development in computing that is currently attracting many practical usages. The main purpose of wireless sensor networks is to observe an area including detecting, identifying, tracking and localizing one or more items of attention to collect data, and then sending back the collected data by using the wireless transmission mode. The WSNs are intended to support time-critical applications which are an important class of services supported by the IEEE 802.15.4 standard [6, 15]. Examples for such kind of applications are control, actuation, and monitoring, where the information is delivered within some deadline. WSNs have some limitations as lower computing power, smaller storage devices, narrower bandwidth and very low battery power [10]. The IEEE 802.15.4 is a standard for short range, low rate-bit and low cost wireless personal area networks. It provides MAC and PHY layers for ZigBee [6]. The IEEE 802.15.4 MAC standard specification describes nodes behavior inside the network. To support time-critical applications, IEEE 802.15.4 uses a Guaranteed Time Slot - GTS allocation mechanism at the network coordinator. The packets are transmitted using a super-frame. Each super-frame is divided into Contention Access Period- CAP, and a Contention Free Period - CFP [6]. The GTS allocation provides communication services to time critical data. It makes guarantees on packets delivery and delivery times to be transmitted to the network coordinator [5].

Ensuring security in WSNs is a challenging task because of various constraints. First, sensor nodes usually have limited resources like - battery power, memory, and computational capabilities. Second, sensor nodes are usually deployed unattended hostile environment and are built without any intrusion detection and prevention in mind.

The purpose of this paper is to give performance analysis of the IEEE 802.15.4/ZigBee-based WSNs under specific DoS attacks, called jamming attacks. The analysis is done using OMNeT++ simulation model for WSN. The effects of the number of attackers and different MAC protocols on throughput, network delay, energy consumption, and network load are inclusively evaluated for simulated scenarios.

The rest of the paper is organized as follow. In section 2,

the paper gives an overview of WSN. The IEEE 802.15.4/ZigBee standard is described in section 3. Section 4 presents the characteristics of commonly used MAC protocols for WSNs. Various types of jamming attacks are described in section 5. In section 6 we report results of our simulation study, and discuss the results. We conclude our paper with section 7.

2 WSNs

WSN consists of a large number of sensor nodes (SNs) wirelessly connected to each other, and base station (BS), which connects the SNs with another network. WSNs are new field of research, which is currently growing rapidly [18].

2.1 WSN Architecture

The specific wireless sensor network structure is presented in Figure 1.

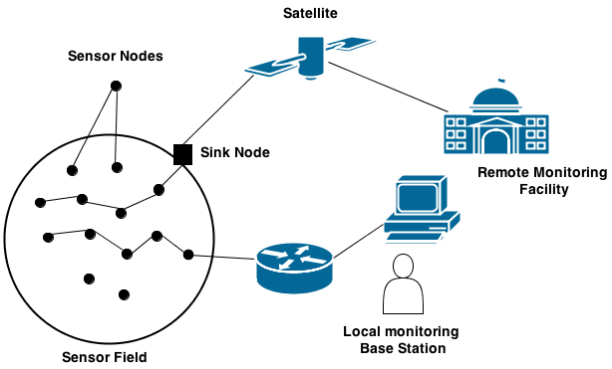

Figure 1. WSN architecture.

Wireless sensor network (WSN) consists of a large number of low power, low cost sensing devices, with light weight and small size, also called motes or nodes, distributed spatially over the physical environments. These nodes are able to form a self-organised network [13]. In the sensor field, the sensed data is collect from the sensor nodes and transmit back to sink node through wireless communication, then sink node forward the sensed data to the users via other communication links (e.g. Satellite) [13]. Sink node can represent different type of device, such as portable computer, PDA (Personal Digital Assistant), or ground station, etc. A sensor node might vary in size, from a shoe box down to the size of a grain of dust or a size of a gold coin [10].

2.2 Characteristics of the WSN

In traditional wireless networks (such as mobile ad hoc networks (MANETs), cellular network, and Bluetooth), wireless nodes are self-organized into an infrastructure networks with dynamic topology [10]. They use the dynamic routing and mobility management technology to achieve the purpose of multimedia data transmissions, for example, voice, images and video. Compared with the traditional wireless network, WSN has many similarities as well as several significant differences, such as the huge number of nodes, limited node hardware resources, power supply constraints, dynamic topology and self-organization, etc. [23]. The primary goal of wireless sensor network is to utilize the energy efficiently. To do this, it is essential to minimize energy use by reducing the amount of communication between nodes. The following are some of the main characteristics and restrictions of wireless sensor network: very small devices, large deployment scale, low cost products, energy efficient function, self-organized, fault tolerance, area coverage, mobility, reliability, flexibility, universality, limited power supply capability and many more [13].

2.3 Factors Affecting the WSN Design

The WSN design is influenced by many factors, which include *reliability*, *scalability*, *production costs*, *network topology*, *operating environment*, *transmission media*, *quality of service and energy consumption* [18]. In the following part of this section, we describe the design factors of protocols and algorithms for WSNs.

2.2.1 Reliability

Reliability or fault tolerance of a sensor node is the ability to maintain the sensor network functionalities without any interruption due to sensor node failure [7]. Environmental interference, physical damage or exhaustive energy source can cause the SN to fail. However, it is important that the failure of a SN does not affect the overall efficiency of the network [18].

2.2.2 Scalability

The number of SNs deployed in studying a phenomenon may be in the order of hundreds or thousands [18]. Depending on the application, the number may reach an extreme value of millions. The new schemes must be able to work with this number of nodes. The density can range from few SNs to a hundred SNs in a region that can be less than 10m in diameter [3].

2.2.3 Production Costs

Since the WSNs consist of a large number of SNs, the cost of a single node is very important to justify the overall cost of the networks. If the cost of the network is more expensive than deploying traditional sensors, then the WSNs is not cost-justified. As a result, the cost of each sensor node has to be kept low [18].

2.2.4 Sensor Network Topology

The network topology affects many characteristics like: latency, capacity, and robustness. Also, the complexity of

data routing and processing depends on the network topology [3]. Paper [2] defined three phases related to topology changes and maintenance: *deployment phase, post-deployment phase and re-deployment phase*. Topology changes during the phase of post-deployment are due to node failures and nodes position changes because of the mobility. During the phase of re-deployment, additional nodes are deployed in the network. This can happen at any time [18].

2.2.5 Operating Environment

SNs are densely deployed either very close or directly inside the phenomenon to be observed. Therefore, they usually work unattended in remote geographic areas. They may be working in busy intersections, interior of large machinery, bottom of an ocean, in a battlefield beyond the enemy lines, large building, attached to animals etc. [18].

2.2.6 Transmission Media

In a multihop sensor network, communicating nodes are linked by a wireless medium. These links can be formed by radio (e.g., Bluetooth compatible 2.4GHz transceiver); infrared which is license free and robust to interference from electrical devices, and optical media [18, 3].

2.2.7 Energy Consumption

The wireless SN can only be equipped with a limited power source. Lifetime of a sensor node depends strongly on the battery life time, especially where no power source replenishment is possible [3]. The main task of a SN in a sensor field is to detect events, perform quick data processing, and then transmit the data. The power resource can be divided into three domains: *sensing, communication, and data processing* [18].

2.2.8 Quality of Service

In some applications (i.e., time constrained applications), one of the big challenges is the data to be delivered within a bounded latency. Otherwise, after certain latency, the sensed data will be useless. In other applications (e.g., not time-constrained applications), the conservation of power is more important than the quality of the sent data [10].

3 IEEE 802.15.4/ZigBee Overview

This section provides a brief overview of the IEEE 802.15.4 standard, with focus on the relevant standard parameters to this study.

The IEEE 802.15.4 is a part of the IEEE family of standards for physical and link-layers for Wireless Personal Area Networks (WPAN) [6].

IEEE 802.15.4/ZigBee is a standard protocol for Low-Rate Wireless Personal Area Networks (LR-WPAN). Its main features are network flexibility, low data rate, low cost and very low power consumption, which make it suitable for an ad-hoc network between inexpensive fixed, portable and moving devices. The IEEE 802.15.4 protocol includes a PHY layer and MAC sub-layer for the LR-WPAN [7]. The PHY layer offers three operational frequency bands; there are a total of 27 channels allocated in the 802.15.4 range, with 16 channels in the 2.4 GHz band, 10 channels in the 915 MHz band, and 1 channel in 868 MHz band [12]. The MAC sub-layer handles all access to the physical radio channel. It provides an interface between the service specific convergence sub-layer (SSCS) and the PHY layer.

3.1 ZigBee Specifications

IEEE 802.15.4 is the foundation of ZigBee network stack architecture, so it directly quotes the PHY and MAC layers from IEEE 802.15.4 standard. The first version of ZigBee standard was released in 2004 by the ZigBee Alliance [10].

Table 1 presents the basic specifications of the ZigBee 802.15.4 standard.

Table 1: Basic ZigBee specifications

Parameters	ZigBee value
Transmission Range (meters)	1 – 100
Battery Life (days)	100 – 1000
Network Size (# of nodes)	> 64.000
Throughput (kb/s)	20 – 250

ZigBee defines two types of equipment: Reduced Function Device (RFD) and Full Function Device (FFD). RFD can only be used as end devices, while FFD can be used as a router, coordinator, and end devices [10]. WPAN is composed of several RDFs, FFDs, or both of them. In the wireless personal area network, each device exchanges data in accordance with WPAN communication protocol. In a PAN, there is at least one FFD as PAN coordinator and each PAN will have a unique ID [12].

The IEEE 802.15.4 can operate either in a Beacon enabled or a non-Beacon enabled mode. The non-Beacon enabled mode is useful for light traffic between the nodes. It uses un-slotted CSMA/CA mechanism [6, 9]. In Beacon-enabled network, the coordinator sends periodic beacons containing information that allows nodes to synchronize with the network, and information on the data pending for the different nodes. In this mode, nodes communicate through a super frame. Each super frame has an active period, during which nodes can communicate using slotted CSMA/CA, and an inactive period during which nodes may turn off the radio in order to conserve energy [9, 19].

Beacon enabled network is usually used for energy efficiency. IEEE 802.15.4 is mainly used in a device which power must be long lasting and has a low network throughput requirement, so that can make it in a very simple and low cost environment to use the wireless network to communicate with other devices [18].

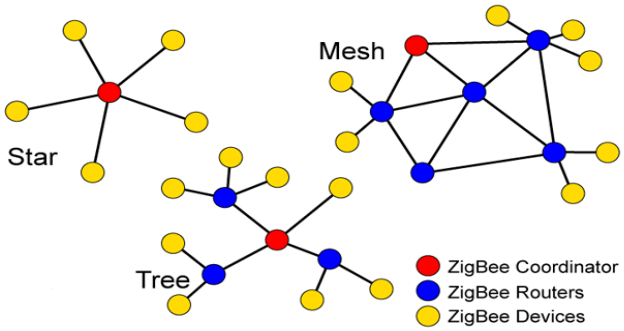

Figure 2. Network topologies

The ZigBee network supports three types of wireless network topologies: Star, Mesh and Tree that can be considered as a special case of Mesh topology (Figure 2).

4 MAC Protocols for WSN

This section introduces the best known MAC protocols for WSNs. A short overview of some important characteristics and features of these MAC protocols are given below.

4.1 Sensor MAC (S-MAC)

The basic idea behind the S-MAC protocol is periodic sleep-listen schedules based on synchronization [8]. S-MAC operates by placing a node in a state that listens to the medium. If there is nothing to hear, node sends a SYNC packet with a schedule defining listen and sleep periods. All nodes hearing this packet will adopt the schedule. Nodes may adopt two or more schedules (if different neighbours have different schedules) [14]. The required period for each node to send a SYNC packet is called *synchronization period*. One important feature of S-MAC is the concept of message-passing, where long messages are divided into frames and sent in a burst [8]. Energy saving can be achieved by minimizing communications overhead. Advantages of S-MAC include sleeping periods, which reduce the energy consumption. The protocol adapts easily on topology changes, and does not use a central entity [14]. Disadvantage of this protocol is that the control frames such as RTS/CTS increase collision probability, generate overhead and increase energy usage [8, 14].

4.2 Timeout MAC

Collision, overhearing, control packet overhead, and idle listening of S-MAC are one of the reasons for improvement of S-MAC protocol. The new enhanced protocol is called T-MAC. In T-MAC, listen period ends when no activation event has occurred for a time threshold [8]. The T-MAC protocol improves on S-MAC by using an adaptive duty cycle. Sensor nodes go to sleep when there is no activity. T-MAC provides a better throughput than S-MAC under variable types of traffic. When the traffic load is heavy, the throughput of T-MAC performs more efficiently than S-MAC. However, the throughputs of both protocols are influenced by packet collisions [4]. An efficient collision avoidance method needs to be developed to decrease the waste of battery energy of sensor nodes and improve the overall network performance,

4.3 Berkeley MAC for Low-Power Sensor Networks (B-MAC)

B-MAC employs an adaptive preamble to reduce idle listening, a major source of energy usage in many protocols [14]. It operates by periodically listening for channel activity. If a channel is sensed to be busy, nodes turn on their receivers, and they turn off after a data packet is received or after certain time out [4]. During transmission, a sender will send a long preamble time period to inform the destination to receive a data packet. But first, the receiver needs to wake up and listen to the channel until the data packet is received. This results in wasting energy. An advantage of using a B-MAC in WSNs is that it does not use RTS, CTS, and ACK, or any other control frame by default. It does not use synchronization, and the protocol performance can be tuned by higher levels to meet the need of various applications [14].

5 Attacks on WSNs

Wireless sensor networks are vulnerable to several key types of attacks. Attacks on WSN can be performed in a variety of ways, most notably as denial of service (DoS) attacks, but also through traffic analysis, privacy violation, PHY attacks etc. [22]. Denial of Service (DoS) attacks, defined as any event that diminishes or eliminates a network capacity to perform its expected function, degrade networks' intended services to its users. [17]. This section discusses most common attacks on WSN on different layers.

5.1 Attacks on the Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [20]. One of the most known attacks on the physical layer is Jamming. Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. Jamming is the type of attack which interferes with the radio frequencies used by sensor nodes and may be viewed as a special case of denial of service (DoS) attacks [21].

5.2 Attacks on the MAC Layer

Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. A collision occurs when two nodes tries to transmit on the same frequency simultaneously. When packets collide, they are discarded and need to be retransmitted. Repeated collisions can also be used by an attacker to cause resource exhaustion [20].

5.3 Attacks on the Network Layer

The network layer of WSN is vulnerable to different types of attacks, such as: spoofed routing information, selective packet forwarding, sinkhole, Sybil, wormhole, blackhole and grayhole, HELLO flood etc.

5.3.1 Spoofed, Altered, or just Replayed Routing Information (also Known as False routing Information)

In this kind of attacks, the primary focus is on the routing protocol. The most direct attack against a routing protocol is to target the routing information in the network [20]. Therefore, by just changing the routing information of the routing protocols through malicious code, it is possible to change the complete routing structure of the Wireless Sensor Network [2].

5.3.2 Selective Forwarding

In a multi-hop network like a WSN, for proper message delivery all nodes need to forward message accurately [11]. Here, the attacker attacks on one of the nodes and infects it with a malicious code which in turn acts just like any other normal node in the WSN, but instead of forwarding the node in the path to the next node, it just drops those packets which make them act as a failed node. Such behaviour would cause problems for the considered WSN [11].

5.3.3 Sinkhole Attacks

During Sinkhole attacks, the attacker's main aim is to tempt all the nodes in close proximity constructing a figurative sinkhole. For example, once the main coordinator is attacked with sinkhole, all of the other nodes will also fall into the sinkhole following the main coordinator as the parent node at the center [11]. Sinkhole attacks naturally works by assembling the attacking node to appear like an ideal node particularly targeting the neighboring nodes. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node [20].

5.3.4 Sybil Attacks

In this kind of attacks the attacker infects a single node in the WSN network with a malevolent code masked with multiple identities. From the WSN perspective, the Sybil attack is effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection [20].

5.3.5 Wormholes

In the wormhole attacks, a malicious node excavates the messages it receives at one end of the network over a separate low-latency channel. Then it repeats messages at a different point in the sensor network. One example of this type of attack is when a source node is passing on data to a destination node and malicious node existing in between the source and destination node selectively forwards the data packets. In order the wormhole attacks to be more effective it usually engage two different and far-away malicious nodes conspire to minimize the distance from each other. They replay packets through out-of-reach channel which is only available to the attacker [11].

5.3 Attacks on the Application Layer

The application layer communication is vulnerable in terms of security compared with other layers. The application layer supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. Main attack at the application layer is attacks on reliability. There are two types of application layer attacks: malicious code attacks and repudiation attacks. *Malicious code attacks:* Malicious code, such as viruses, worms, spywares, and Trojan Horses, attack both operating systems and user applications. *Repudiation attacks:* Repudiation refers to a denial of participation in all or part of the communication [16].

6 Simulation Model and Simulation Results

The tools used for our simulation study are OMNeT++ and MiXiM framework. OMNeT++ is a discrete event simulator for studying protocols for wired and wireless networks. OMNeT++ is designed to model the communication network and distributed systems. In OMNeT++ simulations, the nodes communicate with each other by means of messages. The entities in OMNeT+ are implemented by means of components. The system is modeled by a Network Definition file, known as NED file. The NED file contains the description of network in terms of simple module and compound module. Simple module is the lowest level in hierarchy. The INI file is very important file where all the parameters of the network are defined.

MiXiM is specialized tool developed for wireless and mobile simulations in OMNeT++. It provides detailed models of the wireless channel (fading), wireless connectivity, mobility models, like constant speed, rectangular, circular mobility etc. Also, it provides models for obstacles and many communication protocols mainly at the Medium Access Control (MAC) layer. The specialty of MiXiM is such that its tries to hide the complexity of such simulations and user gets a clean and easy user interface [15].

6.1 Simulation Setup

The simulation model implements MAC and physical layers as defined in IEEE standards. During simulations, IEEE 802.15.4 MAC, S-MAC and T-MAC protocols are considered. The designed system consists of three types of wireless sensor ZigBee nodes, a coordinator, a router and an end device (sensing node).

In this simulation experiment, two different scenarios are created and share the same attributes during the simulation experiment, except the usage of a MAC protocol. The simulation model considered here use a star topology, where the communication takes place between the node coordinator, a router, and the end devices. Each node is powered with two AA batteries, which should be sufficient for long interval of uninterrupted operation. We used different data rates to represent a DoS jamming attack. By adding jammers into the network, we compare the energy consumption in the coordinator of the three protocols. The simulation time is set to 200 seconds. In order to evaluate the performance of the WSN, and to analyze the impact of the DoS jamming attack, we need to measure the performance metrics of the network. Simulation results have been illustrated for performance measures, such as, throughput, network load, network delay, and energy consumption in the coordinator for three different MAC protocols.

Table 2: Simulation parameters

Parameter	Value
Protocol	IEEE 802.15.4 MAC
Simulation time (seconds)	200
Simulation area (meters)	100x100
Mobility Model	Random Waypoint
Mobility speed (m/s)	0.1
Transmit Power (mW)	1.1
Data rate (kbps)	250
Topology	Star
Packet reception power Theirshold (dB)	-95
Packet Size (bits)	2000 (exponential)
Packet Inter-arrival time (seconds)	0.3 (exponential)
Start time (seconds)	10
End time	End of simulation
No. of nodes	20
No. of jammers	2
T-MAC	
Frame time (ms)	610
Activity time-out (ms)	10
Contend time (ms)	9
S-MAC	
Frame time (ms)	610
Active period (ms)	50 - 800
Contend time (ms)	3 - 9
SYNC packets (bytes)	10

Table 2 below shows the simulation parameters used in OMNeT++ simulation in more detail.

Scenarios consist of 20 mobile nodes moving at a constant speed of 0.1 meters per second. Both scenarios are configured with mobility of 0.1 m/s. In order to detect the impact of the attacks, the number of nodes stays constant and the simulation time is 200 seconds. The aim of this simulation experiment is to determine the impact of jamming attacks on WSN. The first scenario (normal) is a standard scenario without any misbehaving node or attack on the network. This scenario is created in order to compare the other scenario and situations and understand the impact of attack and effectiveness of the network.

The second scenario illustrates the Jammer attack on the mobile nodes. This scenario contains 2 jammers that inject unauthorized traffic into the network and affect the WSN that has no specific detection or prevention mechanism against jamming attacks. For this scenario, it is essential to specify a trajectory for mobile nodes to provide mobility where nodes in the network are constantly moving. The main reason for simulating the scenario 1 where no malicious node or jammer were used, is to identify the state of the network under normal conditions and this will help us to compare and differentiate the impact of a jamming attack on the network in later stages. The jammer specifications are illustrated in Table 3. The jammers used in this scenario are mobile jammers that are used to continuously transmit a radio signal in order to inject a specific amount of packages into the network. These jammers are one of the most effective type of jammers, since they drop the throughput of the network at low level, and when are launched, they attack for a long period of time until it runs out of energy.

Table 3: Jammer parameters

Parameters	Value
Transmit Power (W)	0.005
Trajectory	Vector
Jammer Bandwidth	100.000
Jammer Band-base frequency (GHz)	2.4
Pulse width	2.0
Start Time (seconds)	10
End Time (seconds)	End of simulation

6.2 Simulation Results

In this section the behaviour of the network performances is analysed when the network is attacked by two jammers and when there is not attack conducted. For both of this scenarios three MAC protocols are used (802.15.4 MAC, T-MAC ad S-MAC). Additionally, energy efficiency for both scenarios is considered. According to the simulation experiments outcomes, the following results are generated.

Figure 3 shows the average throughput of S-MAC, T-MAC and IEEE 802.15.4 MAC for both scenarios.

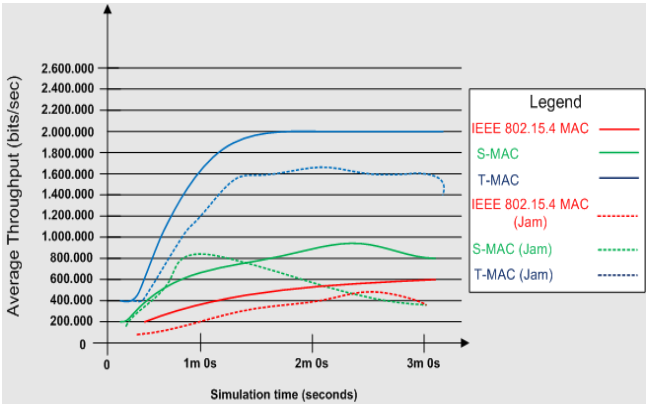

Figure 3: Average Throughput (bits/sec)

Scenario 1 represents the normal scenario without jamming attack and scenarios 2 represents the network that is under DoS (jamming) attack. As we can see in Figure 3, T-MAC provides a much higher throughput than other two protocols, because the traffic loads are distributed into separate wakeup slots. S-MAC achieves insignificant throughput regarding IEEE 802.15.4 MAC, because in S-MAC sensor nodes go to sleep periodically, which is not the case with IEEE 802.15.4 MAC, where each node goes to sleep when the other node is sending. This periodic sleep plays a key role for energy savings. It can be clearly seen that, compared with the normal network state, the jamming attack decreases the overall throughput performance in all three MAC protocols. Because of this, large number of packets does not reach their destination. As in the normal scenario, compared to other two protocols, T-MAC provides significant results when jammers are initialized in the network. S-MAC achieves better throughput instead IEEE 802.15.4 MAC, because of his sending and receiving SYNC packets for periodic listen and sleep.

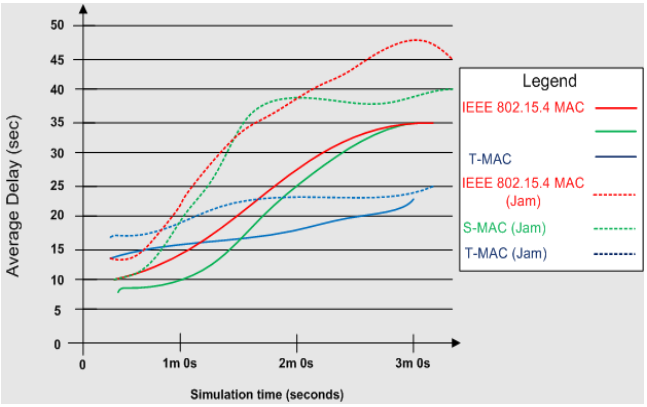

Figure 4. Average delay (sec)

Figure 4 shows the average delay in the network for both scenarios. In normal scenario, the average end-to-end delay when T-MAC protocol is used is less than the delay in other protocols. In S-MAC, the static sleep-listen cycle produces a higher end-to-end delay. IEEE 802.15.4 MAC achieves almost the same delay performance as S-MAC or even better. T-MAC protocol provides a scheme which reduces the collision probability and improves the network delay of data packets. In scenario 2, the reason for the significant difference in delay is the faulty traffic of the attacker which drastically reduces the performance and overloads the network.

This means that, the mobile nodes cannot deliver the packets on time, because of the heavy traffic which is generated by the two jammers. When traffic load is very high (because of the jammers), all packets are generated and queued on the jamming node at the same time, which caused collisions significantly to increase the network delay and retransmission can be done after one schedule interval.

Figure 5 illustrates the average network load for all three MAC protocols, in both scenarios. Best performance achieves T-MAC, because of the active-listen interval, which is long enough to handle to highest expected load. Network load in S-MAC is better than IEEE 802.15.4 MAC, because S-MAC divides time in two parts: active (listening) and inactive (sleeping) part. S-MAC transmits all frames that were queued up during the inactive part, so it shows better load performance. When the jamming attack is launched, the network load level is increased. The jammers generate a heavy traffic, so the network load level will be increased, from the other hand, this will cause a collision in the network and also packet drops.

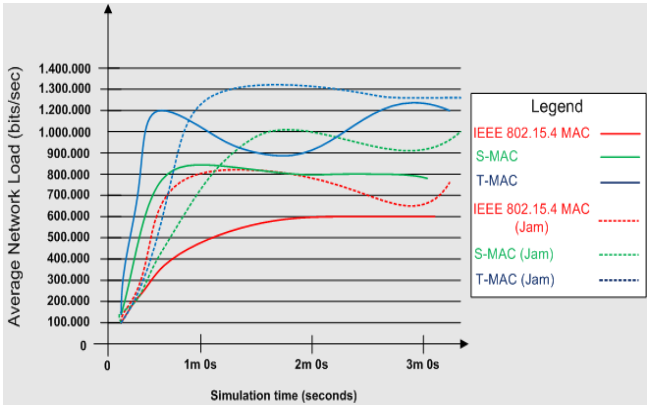

Figure 5: Average network load (bits/sec)

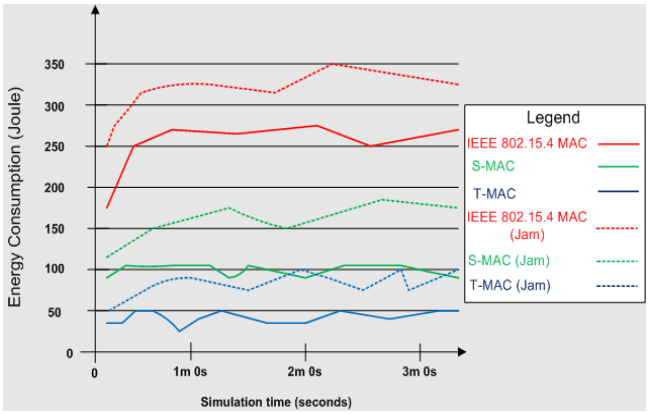

Figure 6: Energy consumption (Joule).

Figure 6 shows the energy consumption by the coordinator in terms of usage of the three different MAC protocols, in normal scenario, and when the network is under attack. T-MAC shows better energy performance due to the introduction to activation time out. S-MAC shows better performance compared to the IEEE 802.15.4 MAC, because of the implementation of SYNC packets. In case of high traffic, S-MAC and T-MAC represent energy savings due to overhearing avoidance. The active time in the frame is longer in the S-MAC, so the energy consumption by this protocol is higher. T-MAC achieves better energy efficiency than S-MAC and IEEE 802.15.4 MAC due to its ability to curtail the active period after completing all transmissions. When the network is under jamming attack, all three protocols shows higher power consumption. However, T-MAC shows better energy efficiency compared to the other protocols even if we compare with the results for S-MAC and IEEE 802.15.4 MAC obtained for the scenario when no attack has been conducted.

7 Conclusion

In this paper, an overview of the wireless sensor networks with special emphasis on the DoS jamming attacks and energy efficiency in WSNs is presented. The IEEE 802.15.4/ZigBee protocol stack offers a practical application solution for low cost, low data rate, and low energy consumption characteristics WSNs. The effect on the network performance using different MAC protocols and the impact of jamming attacks over WSNs has been studied using OMNeT++ simulation software. To evaluate the performance of the WSN and investigate the effectiveness of the proposed MAC protocols, two scenarios are simulated and analyzed. The first scenario is under normal circumstances, and the second one under jamming attack. The attack is conducted by using of two mobile jammers. It is observed that the presence of malicious nodes bring down WSN performance dramatically as jamming attack limits the amount of legitimate sensing data reaching the sink node. The paper analyses four metrics to determine the network performance: throughput, network delay, network load and energy consumption in the coordinator. During the analyses it was figure out that jamming attack decreases the overall throughput in comparison to the normal network state. T-MAC protocol provides a much higher throughput than other two protocols, because the traffic loads are distributed into separate wakeup slots. Under normal conditions, T-MAC provides less end-to-end delay than other protocols; S-MAC shows insignificant results in terms of IEEE 802.15.4 MAC. The average delay during the jamming scenario is higher than the delay during the normal scenario, because of the heavy traffic generated from the jammers. Because of the active-listen interval, which is long enough to handle to highest expected network load, T-MAC achieves best performance compared to other two protocols. The network load level is increased when the jamming attack is launched. The energy consumption in the coordinator is higher when the coordinator is under jammers attack, and the coordinator spent more energy for packets transmission. This leads to decreased coordinator's battery life, and also, shorter network lifetime. The consumed energy by the coordinator for three different MAC protocols is analysed. S-MAC synchronizes the nodes in the network, and use frames where the nodes listen only at the beginning of the active time. T-MAC also operates with frames, but the length of the active time is adapted to the network traffic through simple mechanism. However, T-MAC shows better energy performance compared to the S-MAC and IEEE 802.15.4 MAC, which can be a perfect template to design new high energy efficient MAC protocols and can produce tremendous results.

References

[1] 21 ideas for the 21st century, *Business Week*, pp. 78-167, Aug. 30, 1999.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks (Elsevier)*, vol. 38, pp. 393-422, 2002.

[3] Y. Al-Obaisat and R. Braun, "On wireless sensor networks: architectures, protocols, applications, and management," in *UTSPress*, *Auswireless Conference*, 2006.

[4] Y. C. Chang and J. P. Sheu, "An energy conversation MAC protocol in wireless sensor networks," *Wireless Pers Commun (2009)*, no. 48, pp. 261-276, 2009.

[5] F. Charfi, O. Slama, J. M. Thiriet and S. Lesecq, "Improving the control performance in Wireless Network Controlled Systems, using the Beacon mode," *Journal of Telecommunications*, vol.3, no. 1, June 2010.

[6] F. Charfi and M. Bouyahi, "Performance evaluation of beacon-enabled IEEE 802.15.4 under NS2," *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 3, no. 2, Mar. 2012.

[7] C. Chong and P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," in *Proceedings of the IEEE*, vol. 91, no. 8, Aug. 2003.

[8] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 115-121, 2006.

[9] C. Feng, W. Nan, R. German, and F. Dressler, "Simulation study of IEEE 802.15.4 LR-WPAN for industrial applications," *Wireless Communications & Mobile Computing*, vol.10, no. 5, pp. 609-621, 2010.

[10] Z. Y. Guan, *A Reliability Evaluation of Wireless Sensor Network Simulator: Simulation vs. Testbed*, Master's Thesis – Master of Computing, Unitec Institute of Technology, 2011.

[11] M. Healy, T. Newe, and E. Lewis, "Security for wireless sensor networks: A review," *IEEE Sensor Application Symposium*, New Orleans, LA, USA, Feb 17-19, 2001.

[12] A. Huynh, Z. Jingcheng, Y. Qin-Zhong, and G. Shaofang "ZigBee radio with external power amplifier and low-noise amplifier," *Sensors and Transducers* (1726-5479), vol. 118, no. 7, pp. 110-121, 2010.

[13] A. Jangra, "Wireless sensor network (WSN): architectural design issues and challenges," *International Journal on Computer Science & Engineering*, vol. 2, no. 9, pp. 3089-3094, 2010.

[14] J. Kabara and M. Calle, "MAC protocols used by wireless sensor networks and a general method of performance evaluation," *International Journal of Distributed Sensor Networks*, vol. 2012, 2012.

[15] T. G. Lupu, "Main types of attacks in wireless sensor networks," in *9-th WSEAS International Conference on Signal, speech and image processing*, pp. 180-185, 2009.

[16] A. Khadilkar and N. G. Palan, "Media access control protocol for mobile sensor network-modeling. Using OMNET++ -MiXiM network simulator," *International*

Journal of Computer Science and Information Technologies, vol. 2, no. 3, pp. 1154-1159, 2011.

[17] A. Mehran, Z. Christopher, and A. Afrand, "A game-theoretic approach to security and power conversation in wireless sensor networks," *International Journal of Network Security*, vol.15, no. 1, pp. 50-58, Jan. 2013.

[18] B. Mihajlov and M. Bogdanoski, "Overview and analysis of the performances of ZigBee-based wireless sensor networks," *International Journal of Computer Applications*, vol. 29, no.12, Sep. 2011.

[19] D. Rohm, M. Goyal, H. Hosseini, A. Divjak, and Y. Bashir, "A simulation based analysis of the impact of IEEE 802.15.4 MAC parameters on the performance under different traffic loads," *Mobile Information Systems*, vol. 5, no. 1, pp. 81-99, doi. 10.3233/mis-2009-0074, 2009.

[20] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, no. 2, pp. 55-78, Aug. 2009.

[21] Y. Sun and X. Wang, *Jamming Attacks and Countermeasures in Wireless Sensor Networks*, (Book), doi: 10.4018/978-1-61520-701-5. ch015, pp. 334-335, 2010.

[22] J. Walters and Z. Liang, *Wireless Sensor Network Security: A Survey*, (chapter), Security in distributed, grid, and pervasive computing, CRC Press, 2006.

[23] N. Xu, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A wireless sensor network for structural monitoring," in *2nd International Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA, 2004.

Boris Mihajlov received a B.Sc. from the Faculty of Mathematic and Informatic at Sofia University St. "Kliment Ohridski" – Sofia in 2006, and Master Degree at the European University – Skopje, Macedonia in 2013. His research interests include Wireless Sensor Networks, Information Systems, and Databases.

Mitko Bogdanoski received his B.Sc. degree from the Military Academy, Skopje, Macedonia, and M.Sc. and Ph.D. degree from the Faculty of Electrical Engineering and Information Technologies, Ss Cyril and Methodius University, Skopje, Macedonia, in 2000, 2006 and 2012 respectively. He is an assistant professor at the Military Academy "General Mihailo Apostolski" in Skopje. He is an author of more than 45 international/national conference/journal publications. His research interests include wireless and mobile networks, MANET, WSN, cyber security, energy efficiency and communication theory.