Int. J. Communications, Network and System Sciences, 2015, 8, 29-42
Published Online March 2015 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2015.83004

Scientific Research Publishing

Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite

Arif Sari

Department of Management Information Systems, European University of Lefke, Lefke, Cyprus
Email: asari@eul.edu.tr

Received 26 September 2014; accepted 2 March 2015; published 20 March 2015

Copyright © 2015 by author and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

The 802.15.4 Wireless Sensor Networks (WSN) becomes more economical, feasible and sustainable for new generation communication environment, however their limited resource constraints such as limited power capacity make them difficult to detect and defend themselves against variety of attacks. The radio interference attacks that generate for WSN at the Physical Layer cannot be defeated through conventional security mechanisms proposed for 802.15.4 standards. The first section introduces the deployment model of two-tier hierarchical cluster topology architecture and investigates different jamming techniques proposed for WSN by creating specific classification of different types of jamming attacks. The following sections expose the mitigation techniques and possible built-in mechanisms to mitigate the link layer jamming attacks on proposed two-tier hierarchical clustered WSN topology. The two-tier hierarchical cluster based topology is investigated based on contention based protocol suite through OPNET simulation scenarios.

Keywords

802.15.4 WSN, Communication, Hierarchical Cluster Topology, Simulation, Security, Jamming Attack, Contention-Based Protocols

1. Introduction

Wireless Sensor Networks is very specific type of wireless network regarding to other compared wireless networks. A sensor network contains number of sensor nodes that participates in the network which equipped with specific components such as radio transceiver, specific antenna, a microcontroller, an interfacing electronic circuit and usually a battery or another power source for an energy source. Each participating sensor node sensor

How to cite this paper: Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *Int. J. Communications, Network and System Sciences*, **8**, 29-42.
http://dx.doi.org/10.4236/ijcns.2015.83004

node can be considered as a small computer consisting of a processing unit and a limited amount of computational power and memory. On the deployment of such network, the cost of distributed nodes are relatively low, processing capabilities are low and power consumption should be as low as possible. Since the nodes have mobility feature, the node position is not always known and data rates between nodes during transmission are only few hundred Kbytes/seconds [1]. In addition to this, due to the mobility, the dynamic structure of the network topology rapidly changing. Likewise all other mobile wireless networks, security is one the major problems of WSN due to their dynamic network topology, and lack of centralized infrastructure. The varieties of attacks cause potential threats from different aspects; however, Denial of Service (DoS) is the most harmful attacks against functionality and stability of WSN due to limited resources such as battery and processing power that forces them to be greedy.

The main difference between WSN and MANET is that for WSNs, the main functions are monitoring and collecting the data from the participating sensor nodes for different purposes whereas for the MANET, the main focus is on communication and coordination aspects [1]. Researchers have proposed several defense mechanisms in order to provide security with optimal power and resource consumption. However, lack of security, inconsistency and mobility issues becomes inevitable issues to propose an optimal security solution for WSN [2].

In most of the cases, WSN deployment strategies play significant role on performance of the overall network. Different mechanisms and modifications in routing protocols, or proposing cryptographic key algorithms are quite common solutions for securing mobile or wireless network environments however this is not very suitable due to nature of sensor networks [2].

Deploying the sensor nodes in a controllable manner to achieve maximum network lifetime is the most effective approach of sensor deployment. For that reason, the effectiveness of the implemented deployment strategy relays on a few criteria such as [1];

(a) Range and Coverage
(b) Scalability
(c) Expected Transmission Count (ETX)
(d) Hop Count
(e) Power Consumption

By taking each criterion above into consideration, the deployment model is selected carefully. Each and every criterion plays an important role for performance of entire WSN. In the following sections, the deployment model of the two-tier hierarchical cluster topology model and implemented security model at the link layer will be illustrated. The third section discusses about jamming techniques and different jamming types by illustrating different jamming attacks in WSN. The fourth section discusses about the proposed method and design of the simulation scenario through OPNET 14.5 simulation package. The research paper finalizes with the interpretation of the simulation outcomes in the results and discussions section.

2. Deployment Model

Since the limited resource constraints such as limited power capacity makes WSN sensitive against overhead problems. Researchers have focused on clustering protocols in order to provide minimum connectivity in the network by optimizing energy [3]. The use of cluster heads decreases the amount of complexity and decreases the overall communication overhead on the network. The node adaptation in dynamic topology and control of participant behavior is quite difficult concern to manage in WSN. The cluster based topologies used by variety of researchers in order to measure the network connectivity for energy conservation purposes in the literature [4].

In this section, the basic hierarchical deployment model of the sensor nodes is investigated. The two-tier hierarchical architecture and cluster based sensor classification is discussed. The two-tier hierarchical cluster topology is one of the most common architecture used for WSN.

2.1. Two-Tier Hierarchical Cluster Topology

Clustering the networks is quite efficient and widely used in different types of mobile wireless networks [5]. The two-tier hierarchical cluster topology is one of the most common architecture where larger Wireless Sensor Networks are deployed. This topology is controlled by cluster heads which are separately leads different clusters.

Nodes with specific region send their datagram/segments to a local cluster head where the sensor node belongs. The specific gateway is used to provide communication among different clusters [5]. All cluster heads from different regions and clusters send their collected datagram to the gateway. **Figure 1** below illustrates the deployment model.

In such architectures, cluster heads may send the collected datagram to another region's cluster head where corresponding cluster head would forward the received datagram to the gateway. This topology divides the entire network into small clusters which routing of signals can be done locally so the cluster heads can be designed to be more powerful.

2.2. Characteristics of Cluster Based Sensor Networks

The cluster based sensor networks consist of a cluster head sensor node and cluster member sensor nodes. The cluster head sensor node receives data from the cluster member sensor nodes. All member nodes communicate with cluster head node rather than communicating with other participating sensor nodes in the network or in another cluster [6]-[8]. This leads to an advantage for WSN where minimizes the overhead problem and also minimizes the total energy consumed. **Figure 2** below illustrates the cluster based sensor network working mechanism.

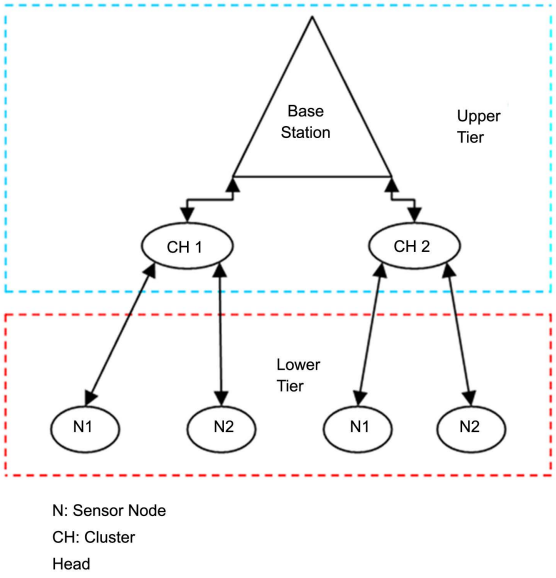

Figure 1. Two-tier hierarchical structure.

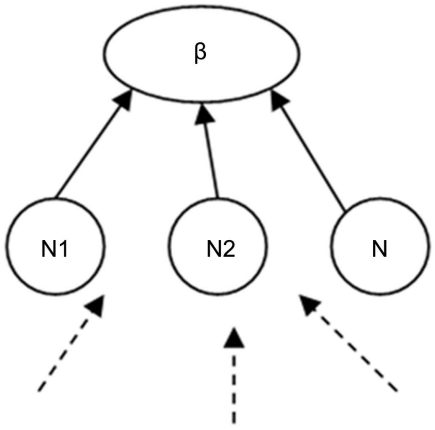

Figure 2. Cluster based sensor network.

Sensor nodes consume less power for communication since all coordination and communication facilities with gateway are provided by cluster head sensor node. The mathematical representation of total energy consumed for communication can be defined as state in Equation (1):

$$\text{Ecom} = 2(\text{N}-1)\text{NPEelectron} + \text{NPE}\,\epsilon\text{f}\;\Sigma = 0\;\text{i},\;\beta,\;2\text{i} \neq \beta \tag{1}$$

On the mathematical representation above, the N is the number of quantization bits that transmitted among sensor nodes to cluster head sensor node, P represents the signal frame length, Eelectron represents the energy consumed for running the electronic circuits and ϵf is used to represent the amplifier energy factor.

Based on the literature survey conducted and information gathered from the researchers investigation on WSN deployment models, the following mathematical representation which are Equation (2) and Equation (3) proves that the cluster based sensor networks are more energy efficient than other network structures.

$$\text{If}\quad \text{M}(\text{N2}-3\text{N})\text{Eelectron} + 2\epsilon\text{f}\,\text{MN}(\text{N}-1)\text{D}\,2/3 + (\text{N2}+\text{P})\text{Ec} > \epsilon\text{mpMN}(\text{D}\,4/5 + 2\text{H2D}\,2/3 + \text{H4}) \tag{2}$$

or

$$\text{If}\quad \text{M}(\text{N}-2)\text{Eelectron} + \epsilon\text{fsM}(\text{N}-1)\text{D}\,2/3 + (\text{N2}+\text{P}-1)\text{Ec} < \epsilon\text{mpmpMN}(\text{D}\,4/5 + 2\text{H2D}\,2/3 + \text{H4}) \tag{3}$$

The throughput calculation is also given through the formula shown in Equation (4);

$$\text{Throughput} = \frac{(\text{Number of delivered packets} \times \text{Packet size})}{\text{Total duration of simulation}} \tag{4}$$

3. Jamming in Wireless Sensor Networks

The jamming attack is one of the most serious problems for Wireless Sensor Networks. This section describes the taxonomy of jamming attacks by classifying the jammers and jamming attack techniques separately with illustrations.

3.1. Jamming Techniques

Basically, jamming is one of the light weight Denial of Service (DoS) type attack which is easy to launch on sensor networks but difficult to detect [9]-[12]. There are 4 types of jamming techniques available in the literature which is illustrated in **Figure 3** below. These are namely Spot Jamming, Sweet Jamming, Barrage Jamming and Deceptive Jamming.

The spot jamming is technique where intruder node transmits all its power to into a single frequency in order to override the original signal. The malicious participant prevents WSN from shifting into another frequency to survive from the attack [9]-[12]. **Figure 4** illustrates the spot jamming attack scenario below.

In the sweep jamming attack aims packet loss and poor data transmission by poisoning multiple frequencies on the network. Attacker aims to increase packet retransmission rate which leads an increase in energy consumption for sensor nodes in the network [9]-[12]. The sweep jamming attack is illustrated on **Figure 5**.

In barrage jamming attack, attacker increasing the range of jammed frequencies. The malicious sensor node has prepared itself jam into group of frequencies simultaneously in the sensor network in order to decrease signal-to-noise ratio of the victim. This attack aims to decrease overall performance of the sensor network [9]-[12]. **Figure 6** illustrats the example of barrage attack.

In deceptive jamming attack is proposed to mislead sensor nodes through false information without exposing themselves on the network. The attacker floods useless data into network and reducing the total available bandwidth for the participant sensor nodes [12] [13].

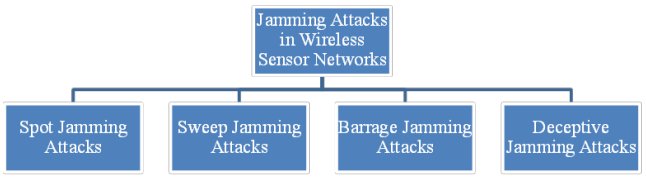

Figure 3. Jamming attacks in WSN.

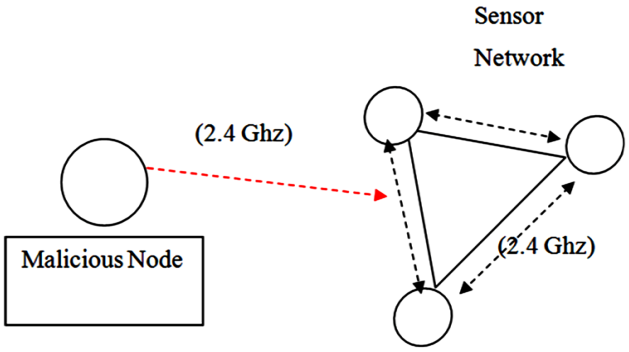

Figure 4. Spot jamming attack.

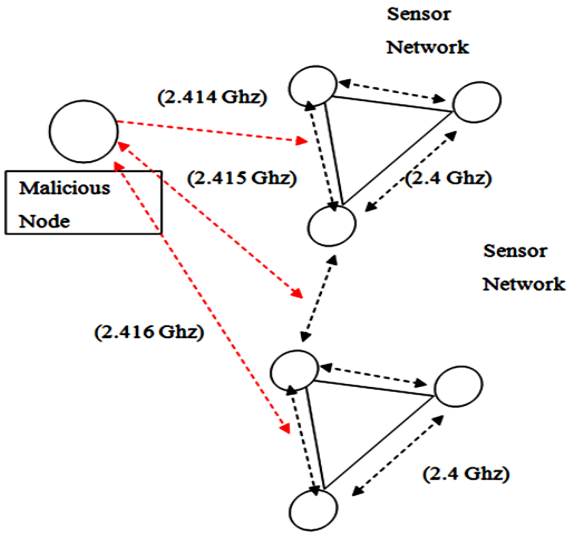

Figure 5. Sweep jamming attack.

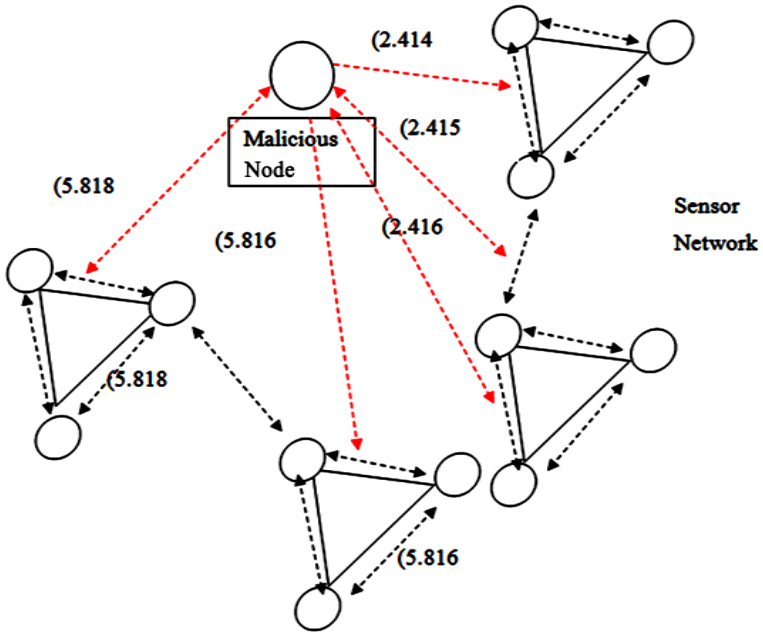

Figure 6. Barrage jamming attack.

3.2. Jammer Types

The jammers are used to launch jamming attacks on sensor networks. This section explains different types of jammers used in different jamming attacks while the basic jamming attacks are stated in the previous section.

There are 4 types of jamming techniques available to use in different jamming attacks as shown on **Figure 7**. These are constant jammer, deceptive jammer, random jammer and reactive jammer.

The constant jammer is the basic jammer type and used to keep entire transmission channel busy to disturb communication between sensor nodes by emitting uninterrupted radio signals on the sensor network [14].

The deceptive jammers are used to mislead sensor network participants by using misleading techniques as proposed in the literature [15].

The random jammers are involved into jamming activities for specific time intervals. These jammers are gets into “sleep” mode and turn back into “wake up” stage randomly and transmit signals [16].

The reactive jammers are more dangerous than the other type since the jammer node listen the activities on the network and transmits a random signal immediately on the detection the legitimate activity in order to disrupt legal communication activities on the network [17]-[19].

4. Proposed Method

The variety of studies conducted on different protocol suites and different protocol layers in 802.11 MANET environment proves that the built-in protocol functionalities have an positive impact on securing the mobile wireless environment while these methods are compared based on specific metrics for better evaluation [20] [21]. The proposed method applied for preventing and mitigating IEEE 802.15.4 physical layer attacks, specifically the jamming attacks at the link layer rather than the physical layer [22]. Due to limited resources and lack of centralized network architecture in WSN, the resources the two-tier hierarchical cluster based deployment model is selected. In such deployment model, a specific base station receives data from cluster head sensor nodes. The proposed method implements the modifications on randomly selected base stations where sensor nodes also behave as base stations on the selected deployment model. The Request to Send/Clear To Send (RTS/CTS) mechanism is so called handshaking mechanism that prevent overhead problem and unnecessary use of “hello” discovery messages on the network [23]. Since the cluster based deployment model is selected for this research, implementation of RTS/CTS mechanism would affect the overall throughput indeed which is used in different mechanisms by the researchers and its impact has proven [24]. The role of CTS mechanism is to silence all wireless stations in its vicinity to avoid collisions and enables the sender of the RTS message to begin data transfer [14]. Such mechanism prevents base stations to receive unexpected and huge amount of data from different resources before authorization of handshaking process. **Figure 8** illustrates the handshaking process between two nodes and proposed CTS mitigates overhead and collision problem. While specific researchers proposed to solve and mitigate impact of jamming attacks on tactical networks and eliminate the collision at the data link layer [24], the jamming attack is investigated at the MAC layer of sensor networks that where collision occurs on “DATA” frames and results to degradation of overall network performance.

The jammers used in this research is constant jammer where continuously emits radio frequency signals in form of random generated packets devoid of any MAC layer protocol or rules [24]. These constant jammers send random and meaningless signals to the communication channel in order to lead collision and overhead on MAC layer protocols. These signals are random bits that do not follow any underlying MAC protocol. When signal is produced by a malicious node, a legitimate node sense that the channel is busy and legitimate node can never get an access to the channel to participate or send/receive data [24]. Additionally, the constant jamming attack can simply corrupt the data which is send by the sender through same communication channel through

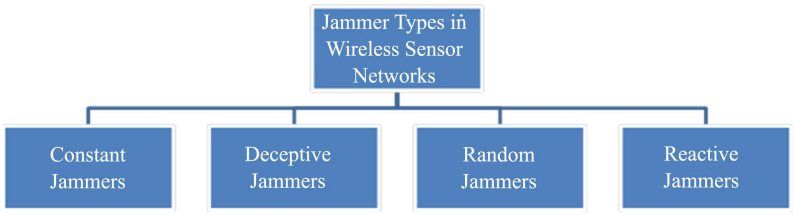

Figure 7. Types of jammers in WSN.

high rate of radio signals. Researchers have proposed different hybrid techniques to detect and mitigate constant jammer attacks and prevent manipulation of communicated data [25]. A wireless Medium Access Control (MAC) protocol is responsible for coordinating transmissions of the nodes on the common transmission medium or shared medium. There are two different algorithms available for contention resolution in IEEE 802.11 working mechanism. These two coordination functions are illustrated in **Figure 9**.

In contention based protocols, such as Carrier Sense Multiple Access/Collision Avoidance protocol (CSMA/CA), when more than 1 wireless access transmitters attempts to access the same channel, the protocol provides reasonable opportunities to transmitters based on some procedures. However, constant jammers don't imply this feature and it does not wait for the channel to be idle before transmitting frames into channel. For that reason, contention based solutions is not possible to implement against such attacks.

The contention-free and contention based protocol suite of the randomly selected base station sensor nodes are modified at the MAC layer according to the proposed model illustrated in **Figure 9**. PCF mechanism is used to coordinate communication in the network. This mechanism uses base station to control all activities in the network. Base station sensor nodes polls the other stations and cluster heads asking them if they have any frame to send.

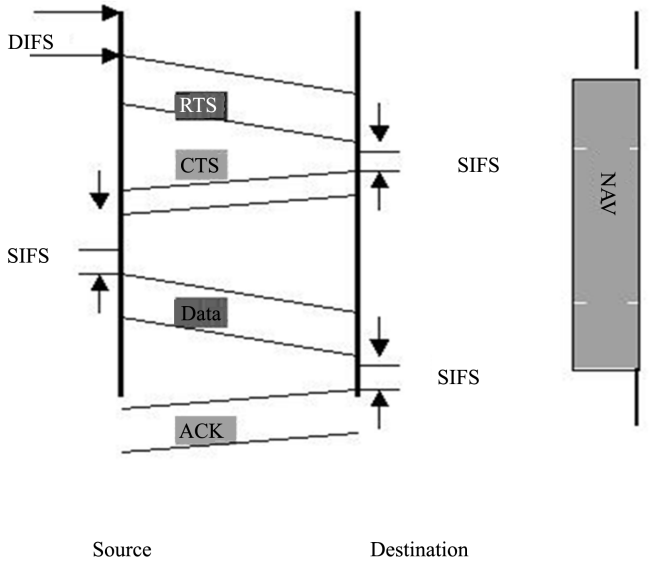

Figure 8. Handshaking/working mechanism in DIFS and SIFS.

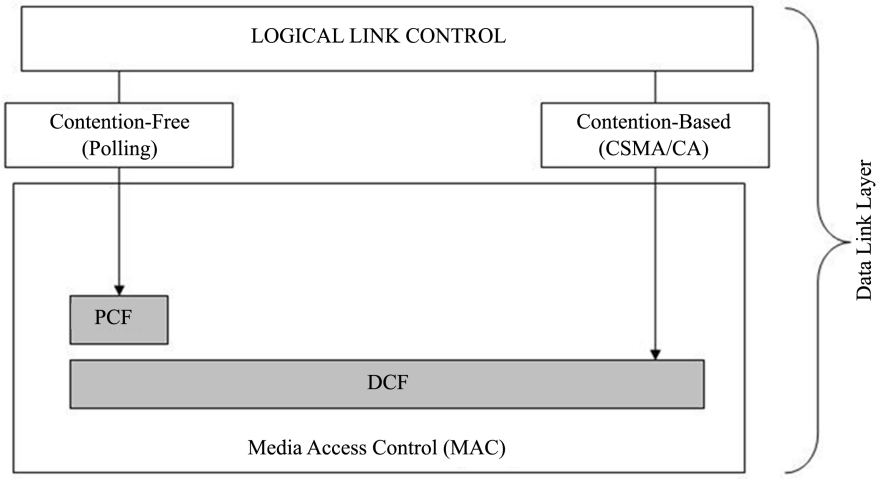

Figure 9. Contention free and contention based protocol structure.

In broadcasts a beacon frames periodically (10 to 100 times per second). The Distributed Control Function (DCF) mechanism is implemented without any modification since PCF mechanism works on DCF. Sensor nodes that use only DCF might not have an access to the shared medium.

Due to priority of PCF over DCF, the repetition interval which is repeated continuously starts with a special control frame called Beacon Frame. When station hears a beacon frame, they start their network allocation vector for the duration of the contention free period of the repetition period [25].

The combination of PCF/RTS-CTS working mechanism is illustrated in **Figure 10**. As it is clearly shown in **Figure 10**, RTS/CTS and PCF mechanism is combined together which is unified security mechanism [14] [18]. The proposed modification done for WSN by combining DCF, PIFS, EIFS, and PCF mechanisms in respect to contention based protocol suite.

The overall performance is expected from implementation of Short InterFrame Spacing (SIFS), PCF InterFrame Spacing (PIFS), DCF InterFrame Spacing (DIFS) and Extended InterFrame Spacing (EIFS). The InterFrame Space (IFS) is defined to provide priority based access to the radio channel. The Shortest InterFrame Space (SIFS) is used for Clear to Send (CTS) and poll response frames [20]. DIFS is the longest IFS and is used as the minimum delay for asynchronous frames contending for access. PIFS is the middle IFS and is used for issuing polls by the centralized controller in the PCF scheme [26]. This model illustrates the combination of RTS/CTS mechanisms with the PCF mechanism to enhance overall network throughput. Guard node model is represented in **Figure 11**.

This node model has modified according to proposed model stated before and transmission radius model is set to 10 meters. Guard node has configured and modified to provide; IKE and static Cyrpto Map sets to increase security on network.

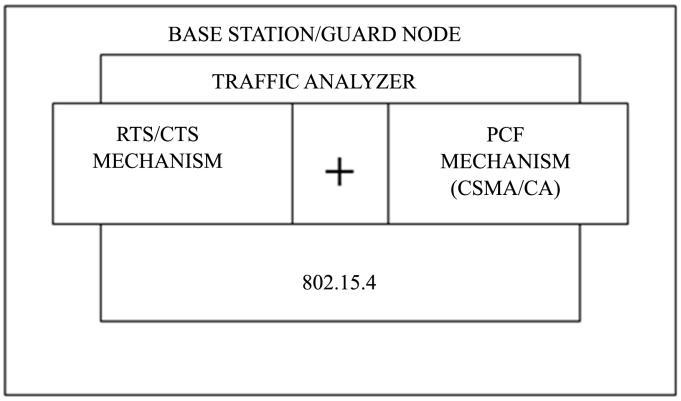

Figure 10. Proposed modification on sensor node.

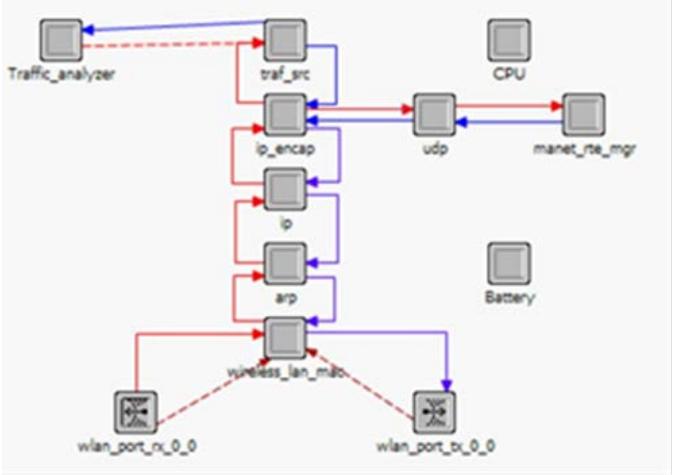

Figure 11. Sensor guard node model.

5. Simulation Model and Experimental Design

OPNET 14.5 simulation package is used for creating WSN scenarios and as a test bed for proposed method. OPNET simulation package provides variety of research and development solutions that helps in research of analysis and improvement of wireless technologies such as Wi-Fi, UMTS, analysis and designing of WSN scenarios, providing power management and scenario design opportunities [27]. In this research, modeling of sensor nodes, clusters and modification of the communication protocol is designed in a specific scenario with specific parameters and global statistics of the scenario is analyzed. **Table 1** indicates the global parameters for simulation scenario.

As it is shown on **Table 1**, parameters are specifically selected to simulate WSN environment with 100 sensor nodes with 2 clusters. Sensor nodes have random waypoint mobility that moves around the area 10 meters/seconds and has automatically configured data rate. In this research, three different scenarios are generated. The first scenario (Scenario 1) contains 100 sensor nodes (divided into 2 satellite subnets) with 1 coordinator and 1 router.

Each cluster has separate cluster head coordinator that controls in-cluster activities and provides communication between sensor nodes of different clusters and use gateway to send data frames. Second scenario (Scenario 2) contains specific mobile jammers which are designed to create constant jamming attack on clusters to disrupt network and consume resources (battery, processing power, network throughput, delay etc.) of sensor nodes and entire network.

In third scenario (Scenario 3), proposed WSN mechanism is implemented on specific sensor node that act as base stations and control points and communicate with main coordinator of the network. There is no difference between the second and third scenario except the implementation of security mechanisms on cluster heads and jammers without changing any other parameters of the scenario. **Figures 12-14** indicate all scenarios and sensor nodes deployed on the network. There are 2 clusters with specific cluster heads that communicate with coordinator.

There are two clusters available in the network that consists of 100 nodes. The main coordinator regulates the coordination between two clusters. The cluster contains subnets where all sensor networks communicate with each other through this subnet as shown in **Figure 12**. The simulation results of this scenario illustrated in the simulation results section of this research as Mobile Discrete event simulation (Mobile DES).

Figure 13 illustrates the simulation scenario consisting of 2 jammers for clusters. There is no guard node exist for in this network. The clusters are under the jamming attack in this scenario. The simulation results are discussed for the corresponding scenario in the next section.

As it is indicated in **Figure 14**, each scenario has 2 clusters with total of 100 sensor nodes. In second scenario, 2 constant jammers are deployed on the network and simulated. The last scenario contains same jammers with combined proposed mechanisms implemented sensor guard nodes to prevent and mitigate the impact of attack.

The global statistics of the simulation scenarios are compared and evaluated in the next section of this research. Performance metrics set as overall network throughput, WLAN Delay and Received/Sent Data over MAC. The impact of the unified security mechanism on WSN is investigated through this test bed.

Table 1. Global simulation parameters for the simulation experiment.

Parameters	Attributes
Protocol	AODV
Simulation Time	1 h
Simulation Area	1000 m × 1000 m
Mobility Model	Random Waypoint
Mobility meters/seconds	10 m/s
Performance Parameters	Throughput, Delay, Traffic Sent/Received
Transmission Power (W)	0.005 W
RTS Threshold	1024
Data Rate	Auto Configured

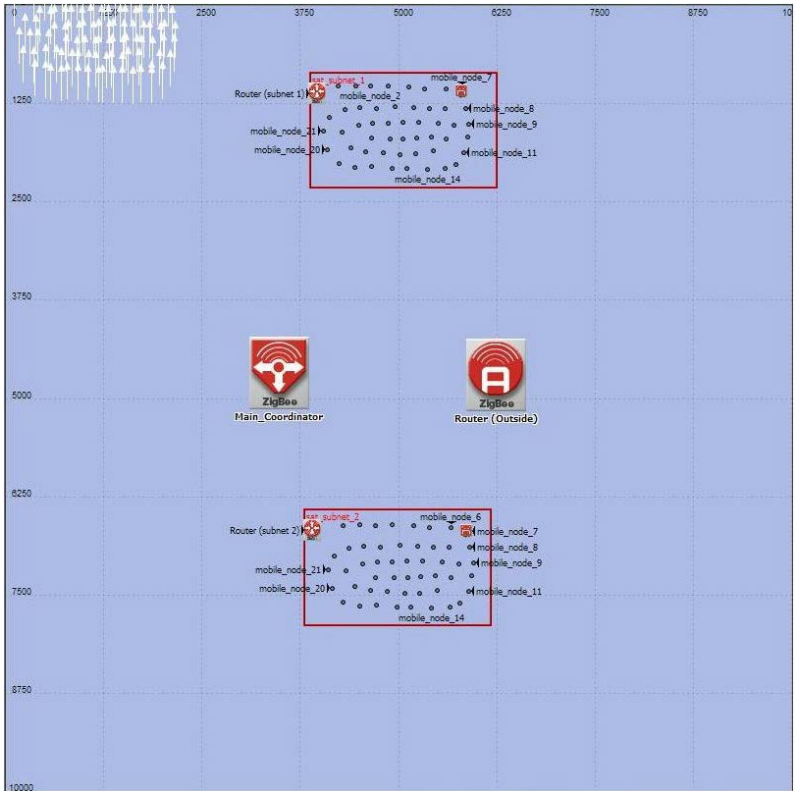

Figure 12. Simulation scenario 1—with no jammers and without guard node.

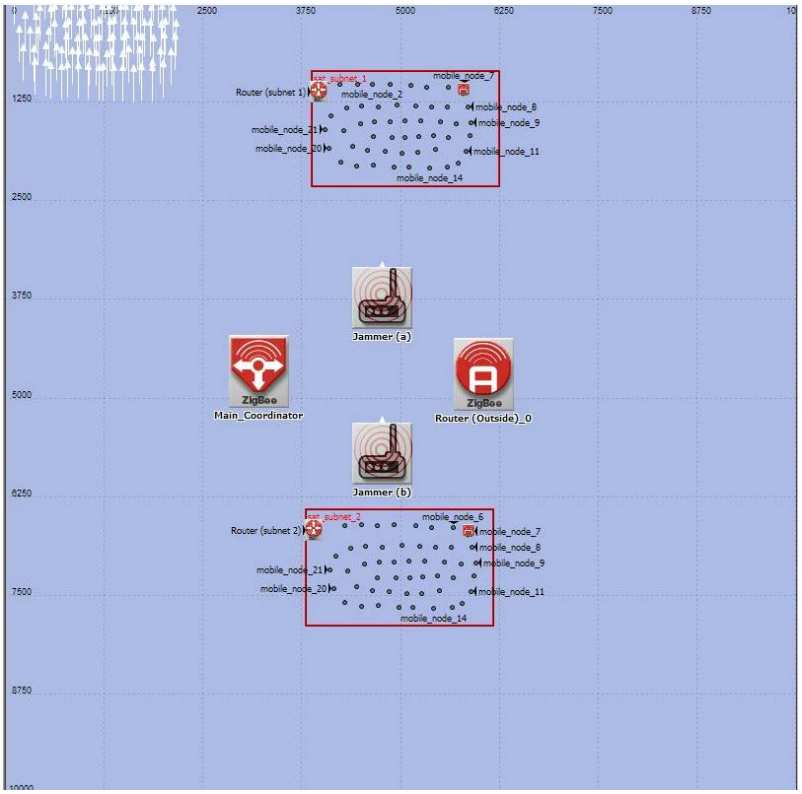

Figure 13. Simulation scenario 2—with jammers and without guard node.

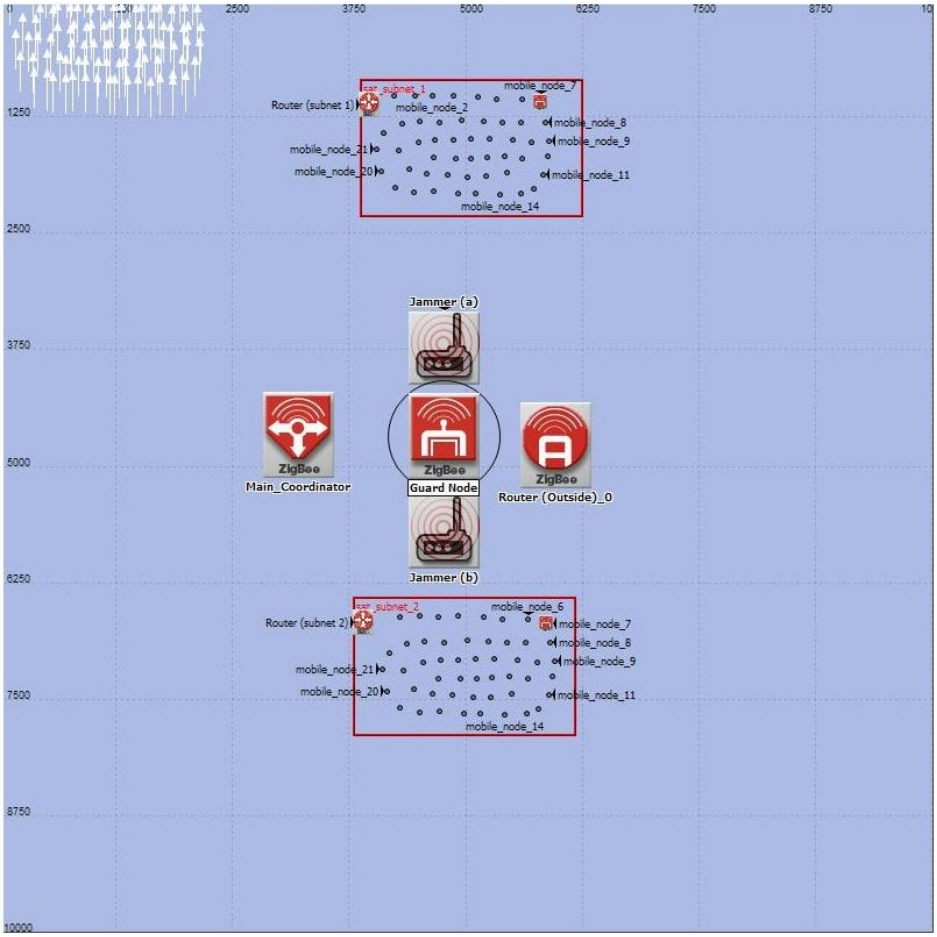

Figure 14. Simulation scenario 2—with jammers and with guard node.

Simulation Results

All scenarios have simulated for 1 hour (60 minutes) for each and every profile. Based on the specific parameters used in this research, MAC Throughput, MAC Delay and MAC Data Traffic Sent/Received parameters are investigated. **Figure 15** illustrates the average MAC Delay for each scenario.

All scenarios are simulated separately to gather 802.15.4 MAC Delay on the network. MAC Delay for Standard Scenario is shown better performance with 0.0173 seconds. In DoS attacker scenario, where the jamming attack is generated, the MAC Delay has shown significant increase with 0.018 seconds while implemented proposed security mechanism improves the MAC Delay to 0.0175 seconds in the short run.

MAC Throughput represents the total number of bits (in bits/sec) forwarded from 802.15.4 MAC to higher layers in all sensor nodes of the network. **Figure 16**, average throughput is analyzed for all scenarios. The average throughput for the standard scenario has shown highest performance with 3000 bits/sec at the beginning of the scenario while diminishing due to high load on the network. In second scenario DoS attack launched on the network and disrupts network performance since the throughput of the scenario has diminished to 1100 bits/sec proposed built-in security mechanism implemented on the third scenario where it improves the throughput of the network from 1100 bits/sec to 2350 bits/sec.

Figure 17 represents the total traffic successfully received by the MAC from the physical layer in bits/sec including retransmissions. The total traffic sent for all scenarios are same since the amount of traffic kept constant. However due to DoS attack launched on the network it leads to a data drop and less amount of data to be received by the MAC layer from physical layer.

The MAC data traffic received represents traffic transmitted by all the 802.15.4 MACs in the network in bits/sec. In **Figure 17**, average data traffic received has shown. The computation of transmitted packets contains

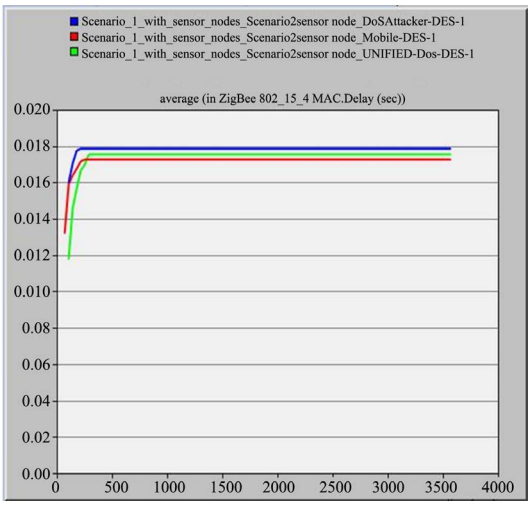

Figure 15. 802.15.4 MAC Delay.

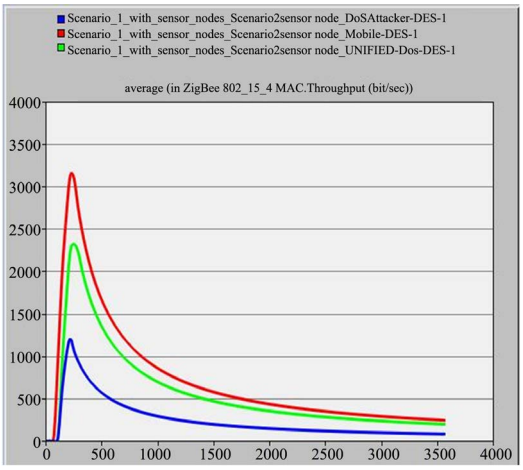

Figure 16. 802.15.4 MAC Throughput.

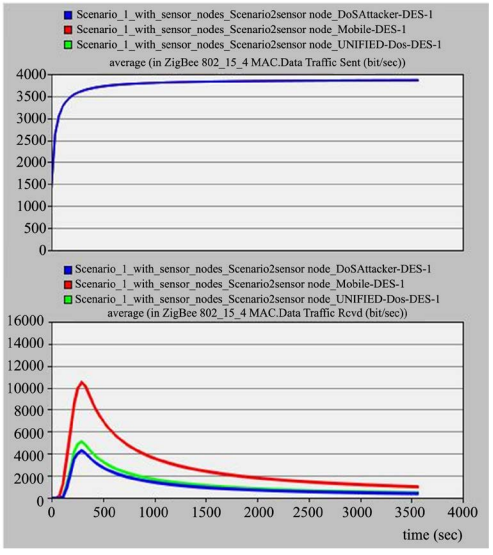

Figure 17. 802.15.4 MAC layer traffic received/sent.

physical layer and MAC headers of the packets. This statistic also represents the impact of CSMA/CA since the statistics include all the traffic that is sent by the MAC via CSMA-CA.

6. Conclusion

In this research combination of built-in mechanisms on IEEE 802.15.4 WSN scenario was simulated and analyzed in OPNET. A specific wireless sensor node model was created and designed to enhance security against jamming attacks on WSN. Global statistic results were obtained in order to analyze the performance of the given network scenario based on set of performance metrics. Comparing total amounts of received/sent transmission packets, we can notice that received traffic at MAC layer is less than that of the built-in security mechanism scenario. That is because data drop rate has increased due to jamming attack on DoS scenario. On the other hand, comparing the throughput among the scenarios, the proposed security scenario throughput shown better performance since the traffic analyzer of the proposed mechanism analyzed the legitimate traffic and permits it to be sent to coordinator instead of allowing the direct flow. The MAC Delay has shown better performance in proposed scenario however the RTS/CTS mechanism might increase the delay in proposed security mechanism and route changes might change the overall performance. The indicators show that, increase in number of proposed guard nodes can increase overall security.

7. Future Recommendations

The flexibility and low-cost of design opportunities of sensor nodes, sensor networks will be very sensitive to radio interference attacks. The mechanisms are proposed to mitigate and prevent jamming attacks. The future work may also have the scope on implementation of guard node selection process in the case of guard node failure indication from MAC layer or sensor node. The guard node selection process or specific guard node deployment model might increase the overall security and performance of the WSN. This novel security system has achieved to prevent physical layer DoS attacks by implementing a specific mechanism on MAC layer.

References

[1] Wood, A. and Stankovic, J. (2002) Denial of Service in Sensor Networks. *IEEE Computer*, **35**, 54-62. http://dx.doi.org/10.1109/MC.2002.1039518

[2] Gurwinder, K. and Rachit, G.M. (2012) Energy Efficient Topologies for Wireless Sensor Networks. *International Journal of Distributed and Parallel Systems* (*IJDPS*), **3**, 179-192.

[3] Virmani, D. and Jain, S. (2013) Cluserting Based Topology Control Protocol for Data Delivery in Wireless Sensor Networks. *International Journal of Computer Science and Issues*, 1-12.

[4] Xu, Y., Bien, S., Mori, Y., Heidemann, J. and Estrin, D. (2008) Topology Control Protocols to Conserve Energy in Wireless *ad Hoc* Networks. CENS Technical Report UCLA, Number 6, Los Angeles, 128-134.

[5] Lee, J.-S. and Chang, C.-C. (2007) Secure Communications for Cluster-Based *ad Hoc* Networks Using Node Identities. *Journal of Network and Computer Applications*, **30**, 1377-1396. http://dx.doi.org/10.1016/j.jnca.2006.10.003

[6] Wu, B., Wu, J., Fernandez, E.B., Ilyas, M. and Magliveras, S. (2007) Secure and Efficient Key Management in Mobile *ad Hoc* Networks. *Journal of Network and Computer Applications*, **30**, 937-954. http://dx.doi.org/10.1016/j.jnca.2005.07.008

[7] Lv, B., Zhang, X.-F., Wang, C. and Yuan, N.-C. (2008) Study of Channelized Noise Frequency-Spot Jamming Techniques.

[8] Xi, Y.-Y. and Cheng, N.-P. (2011) Performance Analysis of Multi-Tone Frequency Sweeping Jamming for Direct Sequence Spread Spectrum Systems.

[9] Murray, S. (1975) Generic Multi-Directional Barrage Jamming System. US Patent No. 3879732.

[10] Schuerger, J. and Garmatyuk, D. (2008) Deceptive Jamming Modelling in Radar Sensor Networks. *Military Communications Conference*, San Diego, 16-19 November 2008, 1-7.

[11] Xu, W., Wood, T., Trappe, W. and Zhang, Y.Y. (2004) Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. *Proceedings of the* 2004 *ACM Workshop on Wireless Security*, ACM, New York, 80-89. http://dx.doi.org/10.1145/1023646.1023661

[12] Sari, A. and Necat, B. (2012) Securing Mobile *Ad-Hoc* Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing* (*IJASUC*), **3**, 79-94.

http://dx.doi.org/10.5121/ijasuc.2012.3306

[13] Law, Y., Hartel, P., den Hartog, J. and Havinga, P. (2005) Link-Layer Jamming Attacks on S-MAC. *Proceedings of the Second European Workshop on Wireless Sensor Networks*, 31 January-2 February 2005, 217-225. http://dx.doi.org/10.1109/EWSN.2005.1462013

[14] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003

[15] Xu, W.Y., Ma, K., Trappe, W. and Zhang, Y. (2006) Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network*, **20**, 41-47. http://dx.doi.org/10.1109/MNET.2006.1637931

[16] Wood, A. and Stankovic, J.A. (2002) Denial of Service in Sensor Networks. *Computer*, **35**, 54-62. http://dx.doi.org/10.1109/MC.2002.1039518

[17] Balogun, V. and Krings, A. (2014) Mitigating Constant Jamming in Cognitive Radio Networks Using Hybrid FEC Code. *IEEE 28th International Conference on Advanced Information Networking and Applications* (*AINA*), Victoria, 13-16 May 2014, 704-711.

[18] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. and Pantziou, G. (2009) A Survey on Jamming Attacks and Countermeasures in WSNs. *IEEE Communications Surveys & Tutorials*, **11**, 42-56. http://dx.doi.org/10.1109/SURV.2009.090404

[19] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile *Ad Hoc* Networks. *International Journal of Science and Advanced Technology* (*IJSAT*), **2**, 188-191.

[20] Wilhelm, M., Martinovic, I., Schmitt, J.B. and Lenders, V. (2011) Short Paper: Reactive Jamming in Wireless Networks—How Realistic Is the Threat? *Proceedings of the Fourth ACM Conference on Wireless Network Security*, ACM, New York, 47-52.

[21] Chen, D., Deng, J. and Varshney, P.K. (2003) Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming. *MOBICOM-Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking*, San Diego, 14-19 September 2003.

[22] Gokhale, V., Ghosh, S. and Gupta, A. (2010) Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks: A Survey. In: Khan Pathan, A., Ed., *Security of Self-Organizing Networks*, MANET WSN WMN VANET, Auerbach Publications, 195-225. http://dx.doi.org/10.1201/EBK1439819197-12

[23] Xu, W., Trappe, W., Zhang, Y.Y. and Wood, T. (2005) The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *MobiHoc* '05: *Proceedings of the 6th ACM International Symposium on Mobile ad Hoc Networking and Computing*, Urbana-Champaign, 25-28 May 2005, 46-57. http://dx.doi.org/10.1145/1062689.1062697

[24] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET. *International Journal of Communications, Network and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[25] Ju, K. and Chung, K. (2012) Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi Hop Tactical Networks. *International Journal of Security and Its Applications*, **6**, 149-154.

[26] Mahajan, R. and Nair, S. (2013) Performance Evaluation of Zigbee Protocol Using Opnet Modeler for Mine Safety. *International Journal of Computer Science and Network*, **2**, 62-66.

[27] OPNET Technologies Inc. "Opnet Simulator". www.opnet.net