A Realistic Modelling of the Sinkhole and the Black Hole Attacks in Cluster-Based WSNs

I. Abasikeleş-Turgut, M. N. Aydin, and K. Tohma
Department of Computer Engineering, Faculty of Engineering, Mustafa Kemal University, Iskenderun, Hatay, Turkey
Email: {iabasikeles, mnaydin, ktohma}@mku.edu.tr

***Abstract*—Due to the positioning in hostile environment, wireless sensor networks (WSNs) are prone to various attacks. Hence, security is one of the most important issues in these networks. Therefore, detecting and preventing several kinds of attacks on WSNs is a popular subject in literature. However, handling these attacks on WSNs requires realistic modeling of these attacks since most of WSNs are application specific. In this paper, two kinds of serious attacks called the sinkhole and the black hole attack are modelled on the LEACH, which is a common cluster-based WSN. Three models are designed for these attacks and the results are evaluated under different performance metrics for different number of nodes. The results show that the black hole attack with a black hole region, which damages the network more than the other attacks, inclines 38% of the packets to be dropped.**

***Index Terms*—black hole, LEACH, sinkhole, wireless sensor network**

I. Introduction

Nowadays, with the gradual maturity of wireless sensor networks (WSNs), they have been widely used in many applications such as battlefield surveillance, smart grid, biomedical health monitoring and habitat monitoring. WSNs consist of many small sensor nodes, which are distributed in open environments without any supervision [1].

Security is one of the most important concepts in WSNs and is crucial for sensor nodes, which are placed in hostile environments, in order to defend against various types of attacks. Designing and applying security protocols for small sensor nodes are challenging work due to their special limitations on energy, computational capabilities, and storage. Therefore, the security mechanism used in sensor networks should vary from the ones used in traditional networks, and be economical in terms of energy, computational and communication overheads [2].

In this context, many researches focused on security issues for WSNs. As a security solution, most of the studies in literature [3]-[6] use cryptographic techniques, which are used to ensure authentication and data integrity by checking the source of the data and verifying that was not altered. However, the main weakness of this approach is its inability to detect accurately insider attacks when the attacker knows the keys and use them to encrypt and decrypt the communication messages [7].

The insider attackers are severely destructive to the functioning of a network [8]. An important form of insider attack in WSNs is the sinkhole attack [9], while one of the major and the most serious insider attacks is the black hole attack [10].

In a black hole attack, the attacker swallows all the messages he receives, just as a black hole absorbing everything passing by. By refusing to forward any message he receives, the attacker will affect all the traffic flowing through it. In a sinkhole attack, given certain knowledge of the routing protocol in use, the attacker tries to attract the traffic from a particular region through it [11].

There are plenty of studies in literature to detect the sinkhole and the black hole attacks in WSN [12]-[15]. However, the concept of "intrusion" is not clear in these networks. Therefore, it is very important to study realistic attacker models and evaluate the practicality and efficiency of certain attacks [16]. Accordingly, in recent years, the studies about modelling the insider attacks have gained acceleration [16]-[18].

In this paper, the sinkhole and the black hole attacks are modelled on the LEACH (Low-Energy Adaptive Clustering Hierarchy) [19], which is often used in literature since it is the basis of the cluster-based algorithms. Three models are designed for the attacker node by using simulation method on OMNeT++. The system is simulated for different number of nodes from 80 to 120 and examined over various performance parameters, such as total energy consumption, the packet loss rate and the number of living nodes. The results show that the malicious nodes lead to packet loss from 7% to 38%. A black hole attack with a black hole region inclines the most damage on the network, while the effect of all attacks decreases as the number of nodes increases.

The simulation framework, the system parameters and the models of the sinkhole and the black hole attacks are summarized in Chapter 2, while the simulation results are discussed in Chapter 3. Chapter 4, which is the last chapter, concludes the paper.

II. Evaluation Methodology

A. Simulation Environment

OMNeT++ is an extensible, modular, component-

Manuscript received January 4, 2015; revised April 14, 2015.

©2016 Int. J. Electron. Electr. Eng.

doi: 10.18178/ijeee.4.1.74-78

based C++ simulation library and framework, primarily for building network simulators [20]. Since OMNeT ++ has a generic architecture it can be used in various problem domains, such as modeling of wired and wireless communication networks, modeling of queueing networks and modeling of multiprocessors and other distributed hardware systems.

In this paper, OMNeT++ is used to model the sinkhole and the black hole attacks on the LEACH, which is a cluster-based routing algorithm (Fig. 1). The LEACH has three basic components called the base station (sink), the cluster head and the sensor nodes [19]. The sink is responsible from evaluating the data, which is gathered from the cluster heads. The sensor nodes transmit their data to the cluster head, while the cluster head node receives data from all the cluster members, performs signal processing functions on the data, i.e. data aggregation, and transmits data to the remote sink.

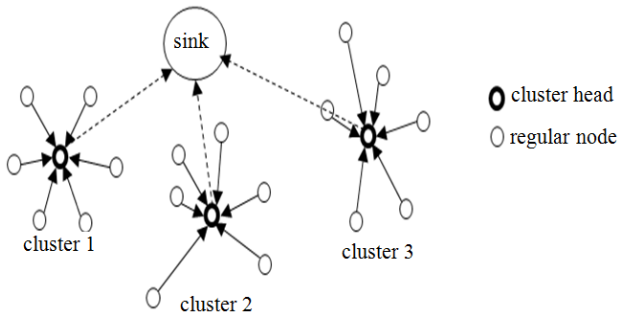


Figure 1. The LEACH: A cluster-based routing protocol for WSNs.

The LEACH is a clustering-based protocol that utilizes randomized rotation of local cluster base stations (cluster-heads) to evenly distribute the energy load among the sensors in the network. The LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station [19].

B. Modelling the Sinkhole and the Black Hole Attacks

In a black hole attack, once the attacker node receives the packets, it drops all of them leading to loss of information [21], while in a sinkhole attack; the attacker tries to attract the traffic through it [11]. In this paper, two different models are designed for the black hole attack and one model is designed for the sinkhole attack.

1) Model-1: *A black hole attack with malicious nodes:*

In this model, the attackers, i.e. malicious nodes, are some of the nodes in the network that have more initial energy than the regular nodes. If an attacker becomes a cluster head in a round, he does not send the packets received from his member nodes, to the sink. From this point of view, this model is similar to the model designed in [21]. In this paper, the malicious node can also be a regular node and does not send his sensed data to the base station. In brief, the malicious nodes can both be cluster heads and regular nodes. In either case, they do not transmit their data to the sink. A malicious node acting as a cluster head and a regular node in Model-1 can be seen in Fig. 2.

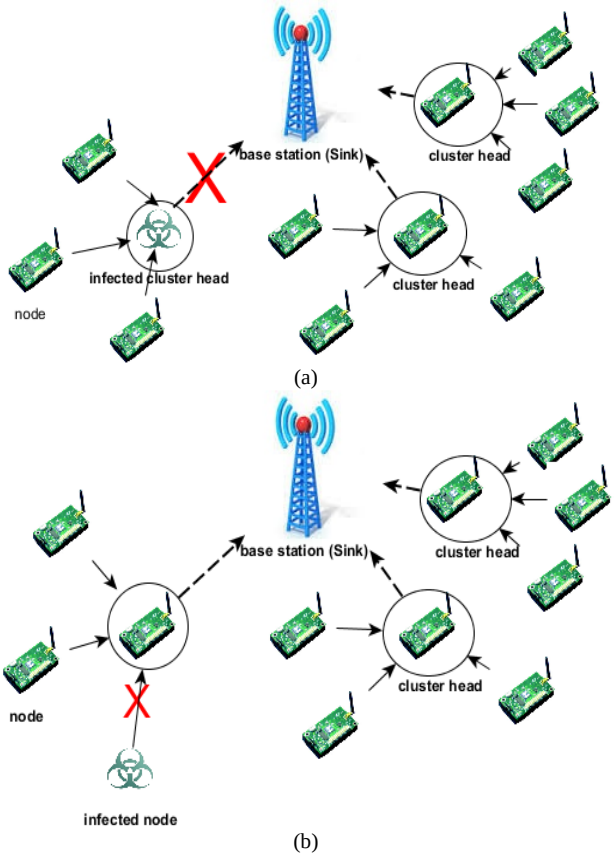
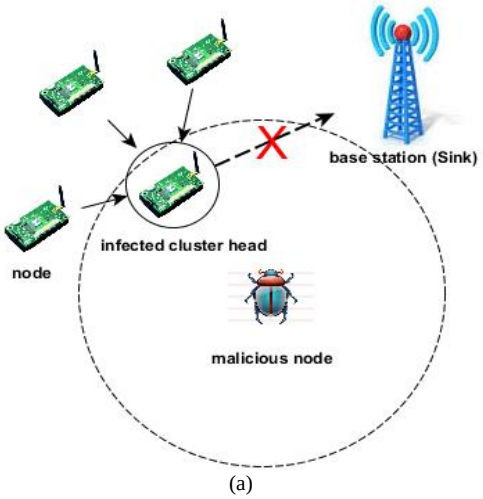
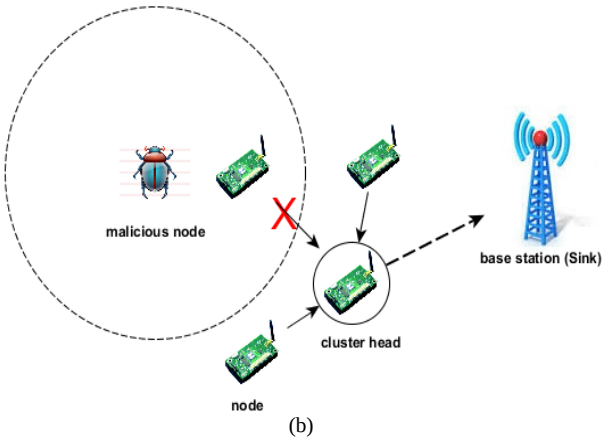


Figure 2. A malicious node acting as a cluster head (a) and a regular node (b) in model-1.

2) Model-2: A black hole attack with a black hole region

In this model, the malicious node, which has a high transmission range to attract the other nodes, is preconditioned in a fixed point in the network. If a cluster head falls into his region in a round, he captures the cluster head and restrains it from sending the data of the cluster member nodes to the sink. Otherwise, if a cluster head does not fall into his region, then he captures the regular nodes and restrains them from sending their sensed data to their cluster head. Fig. 3 shows how the malicious node in Model-2 poisons a cluster head and a regular node.





(b)

Figure 3. A malicious node poisoning a cluster head (a) and a regular node (b) in Model-2

3) Model-3: A sinkhole attack with a malicious node

In this paper, a random node in the network is selected as a malicious node. In a sinkhole attack, the malicious node not only drops the packets, but also tries to attract the traffic through him. Therefore, this malicious node elects him as a cluster head on every round and broadcasts a false advertisement message to the network. After he collects the sensed data from his member nodes, he drops the packets and does not send them to the sink. Since the regular nodes select their cluster head according to the Euclid distance, the position of the sinkhole node play a crucial role on his damage. The malicious node in Model-3 can be seen in Fig. 4.

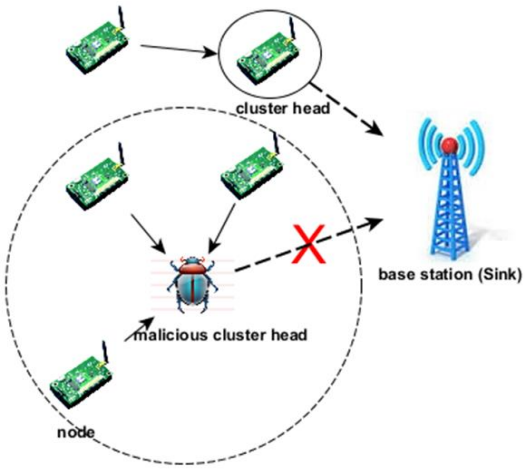


Figure 4. The malicious node is attracting the traffic in Model3.

C. Simulation Parameters

The simulation parameters used in this paper is shown in Table I. As is seen in table, the sink is positioned at the center of an 800m ×800m network area, while 80, 100 and 120 sensor nodes are randomly spread on this network. The malicious nodes in Model-1, the number of which is 10% of total system nodes, have two times more initial energy than a regular node and randomly distributed in the network. The position of the malicious node in Model-2 is (500,500), while the malicious node position in Model 3 is (350,350). The influence area of both Model-2 and Model-3 is 10% of total network area.

TABLE I. SIMULATION PARAMETERS

Parameters	Values
Network Area	800m ×800m
Number of nodes	80, 100, 120
The position of the sink	(400,400)
The percentage of the number of malicious nodes in Model-1	10%
Initial energy of malicious nodes in Model-1	2x x: initial energy of regular nodes
Malicious Node Distribution in Model-1	Random
The malicious node position in Model 2	(500,500)
Influence area of the malicious node in Model-2	10%
The malicious node position in Model 3	(350,350)
Influence area of the malicious node in Model-3	10%

III. RESULTS AND DISCUSSION

The system is simulated under three different attack models, which are discussed above and the results are compared with LEACH under different performance metrics including the number of packets arrived at the base station, the number of living nodes and average energy consumption.

The number of packets arrived at the base station signifies that how many packets succeeded to reach the base station at the end of a round from among the packets generated by all of the regular nodes in the beginning of the round. The number of living nodes states the number of nodes, which have enough energy to continue sensing and communication on the next round, i.e. alive nodes. Average energy consumption is average of energy consumed on every round by all of the nodes due to the transmitting their packets to the base station or cluster head.

Owing to the randomized nature of LEACH, the simulations are executed ten times for each number of nodes under all attack models and average values of the results are calculated for a realistic evaluation. Besides, on the purpose of preventing the figures from being overcrowded, average values of all rounds are demonstrated for every performance metrics. Therefore, average increase in the number of living nodes, average decrease in the number of packets arrived at the base station and average decrease in total energy consumption under three attack models for 80, 100 and 120 nodes can be seen in Fig. 5, Fig. 6 and Fig. 7, respectively.

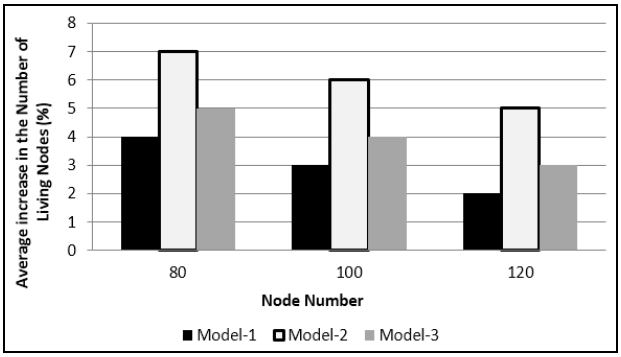


Figure 5. Average increase in the number of living nodes under three attack models for 80, 100 and 120 nodes.

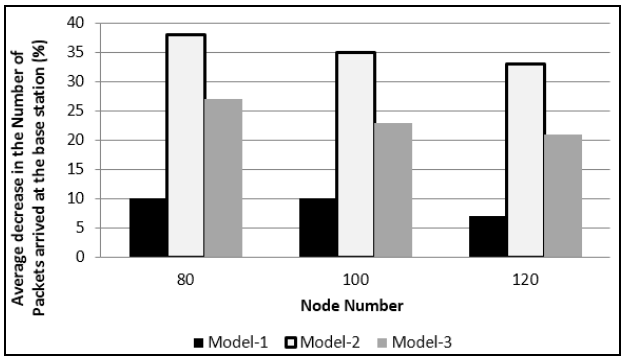


Figure 6. Average decrease in the number of packets arrived at the base station and average decrease in total energy consumption under three attack models for 80, 100 and 120 nodes.

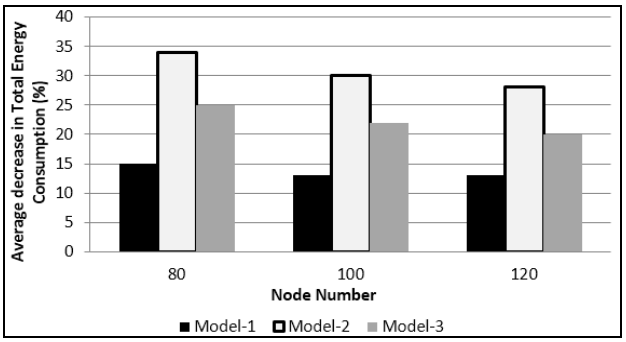


Figure 7. Average decrease in total energy consumption under three attack models for 80, 100 and 120 nodes.

As is seen in Fig. 5, the number of living nodes under all attack models is more than the number of living nodes without any attack. Besides, total energy consumption under all attack models is less than that of without any attack as is seen in Fig. 7. These results can be seen unreasonable at first glance. It can be thought that the malicious nodes provide long network lifetime by increasing the number of living nodes and decreasing the energy consumption. However, the actual reason of these results is not originated from the performance increase; it is why the malicious nodes prevent the packets to arrive at the base station. Thus, the regular nodes or the cluster heads become idle and due to not consuming energy for packet transmission, they can live longer time in the network. The proof of this explanation can be seen in Fig. 6. The number of packets arrived at the base station decreases for all number of nodes under all attacks varying from 7% to 38%.

The damage of attacks can be evaluated from the packet loss rates. As is seen in Fig. 6, Model 2 inclines the most damage with the rates between 33% and 38% for all number of nodes, while Model 3 is hard on the heels of it with the rates between 21% and 27%. Minimum packet loss rates, which are even less than one third of Model-2, are observed under Model-1. The more number of poisoned nodes leads to the more packets to be dropped or lost. Therefore, the effect of models depends on the number of infected nodes. The number of malicious nodes corresponds to the number of infected nodes in Model-1 and is a fixed number of 10% of total nodes. However, the number of infected nodes depends on the action radius of malicious nodes as well as their number. Accordingly, Model-2 and Model-3 poisons larger number of nodes than Model-1. The role of the infected nodes is as important as the number of them. Infecting a regular node causes his packets to be dropped, while infecting a cluster head causes all packets of his cluster member nodes to be dropped. Therefore, infecting a cluster head brings on more damage to the network than a regular node. Wherefore the malicious node in Model-3 acts as a cluster head, he can only poison regular nodes. However, the malicious node in Model-2 infects all of the nodes in his region, including cluster heads as well as regular nodes. In consequence, the packet loss rates have highest values under Model-2.

As is seen from Fig. 5 through Fig. 7, the effect of attacks decreases as the number of nodes increases. The reverse of this effect can be expected. The more number of nodes means the more number of malicious nodes in Model-1 and the more number of infected nodes in other models because the larger number of nodes is positioned in the same network area. In fact, the number of infected nodes increases as the number of network nodes increases. However, the percentage of the number of infected nodes to the number of healthy system nodes decreases and accordingly the damage of the attacks decreases as the number of nodes increases.

IV. Conclusion

WSNs are prone to various attacks because they are usually located in hostile environments. This situation has raised the security to become one of the most important issues in WSNs and plenty of studies to be proposed on it.

WSN security attacks can be classified into two classes called the insider and the outsider attacks. The sinkhole and the black hole attacks are two of the most dangerous insider attacks.

Designing a realistic model for security attacks plays an important role in detecting or preventing them. Therefore, in this paper, the sinkhole and the black hole attacks are modelled. Three models are designed and simulated on LEACH, which is the basis of cluster-based WSNs, by using OMNeT++.

The results show that the black hole attack with a black hole region inclines the most damage with the rates between 33% and 38% for all number of nodes, while the sinkhole attack is hard on the heels of it with the rates between 21% and 27%. Minimum packet loss rates are observed under the black hole attack with malicious nodes. Besides, the effect of all attacks decreases as the number of nodes increases.

References

[1] G. Han, X. Li, J. Jiang, L. Shu, and J. Lloret, "Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks," *The Computer Journal*, May 13, 2014.

[2] S. Hamedheidari and R. Rafeh, "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks," *Computers and Security*, vol. 37, no. 3, pp. 1-14, 2013.

[3] M. Ebrahim and C. W. Chong, "Secure force: A low-complexity cryptographic algorithm for wireless sensor network (WSN)," in *Proc. IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, 2013, pp. 557-562.

[4] K. Rajendiran, R. Sankararajan, and R. Palaniappan, "A secure key predistribution scheme for WSN using elliptic curve cryptography," *ETRI Journal*, vol. 33, no. 5, pp. 791-801, 2011.
[5] S. B. Sasi, D. Dixon, and J. Wilson, "A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security," *IOSR Journal of Engineering*, vol. 4, no. 3, 2014.
[6] L. B. Oliveira, *et al.*, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 485-493, 2011.
[7] A. Abduvaliyev, S. Lee, and Y. K. Lee, "Energy efficient hybrid intrusion detection system for wireless sensor networks," in *Proc. International Conference on Electronics and Information Engineering (ICEIE)*, Aug. 2010, vol. 2, pp. 25-29.
[8] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proc. INFOCOM*, May 2007, vol. 7, pp. 1937-1945.
[9] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-Count monitoring: Detecting sinkhole attacks in wireless sensor networks," in *Proc. 15th IEEE International Conference on Networks*, Nov. 2007, pp. 176-181.
[10] D. Virmani, M. Hemrajani, and S. Chandel, "Exponential trust based mechanism to detect black hole attack in wireless sensor network," arXiv preprint arXiv: 1401.2541, 2014.
[11] K. Xing, S. S. R. Srinivasan, M. Jose, J. Li, and X. Cheng, "Attacks and countermeasures in sensor networks: A survey," in *Network Security*, Springer US, 2010, pp. 251-272.
[12] D. Sheela, *et al.*, "Detecting black hole attack in wireless sensor network using mobile agent," in *Proc. International Conference on Artificial Intelligence and Embedded Systems*, Singapore, 2012, pp. 45-48.
[13] J. Kaur and B. Kaur, "BHDP using fuzzy logic algorithm for wireless sensor network under black hole attack," in *Proc. IJARCSMS*, 2014, vol. 2, pp. 142-151.
[14] D. Sheela, K. C. Naveen, and G. Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks," in *Proc. International Conference on Recent Trends in Information Technology (ICRTIT)*, Jun. 2011, pp. 527-532.
[15] F. J. Zhang, L. D. Zhai, J. C. Yang, and X. Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks," *Procedia Computer Science*, vol. 31, pp. 711-720, 2014.
[16] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks: The intruder side," in *Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2008, pp. 526-531.
[17] S. Iqbal, S. P. A. Srinivas, G. Sudarshan, and S. S. Kashyap, "Comparison of different attacks on LEACH protocol in WSN," *İnternational Journal of Electrical, Electronics and Data Communication*, vol. 2, no. 8, pp. 16-19, 2014.
[18] S. Ramachandran and V. Shanmugam, "Performance comparison of routing attacks in MANET and WSN," *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, vol. 3, no. 4, 2012.
[19] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient communication protocol for wireless microsensor networks," in *Proc. The 3rd Annual Hawaii International Conference on System Sciences*, 2000.
[20] OMNeT++. [Onine]. Available: http://www.omnetpp.org/
[21] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," *Procedia Computer Science*, vol. 19, pp. 1101-1107, 2013.

Ipek Abasıkeleş-Turgut was born in Adana, in 1985. She has completed her elementary education at Celalettin Seyhan Primary Education School. She went to ÇEAŞ Seyhan Anatolian High School for her high school education and graduated from there with 1st degree in 1999. Then she deserved to educate in Adana Science School. She has completed her university education at the department of Computer Engineering of Istanbul Technical University (ITU) with a degree of magna cum laude in 2007. She has received her MSc in Computer Engineering and her PhD in Electrical and Electronics Engineering from Çukurova University in 2009 and 2013, respectively.
She worked as an expert computer engineer at Presidency of Çukurova University from 2007 through 2012 and as a Research Assistant at Adana Science and Technology University from 2012 through 2013. Since 2014, she has been working as an Assist. Professor. Dr. at Mustafa Kemal University.
She currently has 2 books, 3 SCI journal papers, 2 national and 4 international conference papers. Her interest areas are wireless sensor networks, parallel processing, simulation and modeling of multiprocessors with distributed shared memory.

Merve Nilay Aydın was born in Osmaniye in 1989. She has completed her elementary education at Cebeli Bereket Primary Education School. She went to Atatürk High School for her high school education. She has completed her university education at the department of computer Engineering of Fırat University in 2011. She has studying her MSc in department of informatics at Mustafa Kemal University since 2013. She has been working as a research assistant at Mustafa Kemal University since 2013. Her interest areas are networks and wireless sensor networks.

Kadir Tohma was born in Hatay, in 1990. He has completed his elementary education at Bedii Sabuncu Primary Education School. He went to Osman Otken Anatolian High School for his high school education. He has completed his university education at the department of Computer Engineering of Cukurova University in 2013. He has studying his MSc in department of informatics at Mustafa Kemal University since 2014. He has been working as a research assistant at Mustafa Kemal University since 2014. His interest areas are networks and wireless sensor networks.