Turkish Journal of Electrical Engineering and Computer Sciences

Volume 24 | Number 5 Article 81

1-1-2016

The impact of disabling suspicious node communications on network lifetime in wireless ad hoc sensor networks

ZEYDİN PALA

NİHAT İNANÇ

Follow this and additional works at: https://journals.tubitak.gov.tr/elektrik

Part of the Computer Engineering Commons, Computer Sciences Commons, and the Electrical and Computer Engineering Commons

Recommended Citation

PALA, ZEYDİN and İNANÇ, NİHAT (2016) "The impact of disabling suspicious node communications on network lifetime in wireless ad hoc sensor networks," *Turkish Journal of Electrical Engineering and Computer Sciences*: Vol. 24: No. 5, Article 81. https://doi.org/10.3906/elk-1411-198
Available at: https://journals.tubitak.gov.tr/elektrik/vol24/iss5/81

This Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Electrical Engineering and Computer Sciences by an authorized editor of TÜBİTAK Academic Journals. For more information, please contact academic.publications@tubitak.gov.tr.

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2016) 24: 4429 – 4444
© TÜBİTAK
doi:10.3906/elk-1411-198

The impact of disabling suspicious node communications on network lifetime in wireless ad hoc sensor networks

Zeydin PALA[1,*], **Nihat İNANÇ**[2]
[1]Department of Computer Engineering, Faculty of Engineering and Architecture, Muş Alparslan University, Muş, Turkey
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, Kırıkkale University, Kırıkkale, Turkey

Received: 29.11.2014 • **Accepted/Published Online:** 07.08.2015 • **Final Version:** 20.06.2016

Abstract: In wireless sensor networks (WSNs), the data observed by different nodes must be relayed safely to the base station over intermediate nodes. In the network environment, some sensor nodes can act suspiciously when they enter someone else's control or due to other equipment failure. Data packets that are sent through suspicious nodes may be randomly dropped or may be not delivered as desired. In this paper, we investigate the impact of disabling suspicious nodes communications on network lifetime through a linear programming framework. We build a mathematical programming framework and perform comprehensive numerical analysis. Our results show that the decrease in WSN lifetime is less than 8.0% if the number of suspicious nodes is not higher than 10%.

Key words: Network lifetime, linear programming, suspicious sensor nodes, wireless ad hoc sensor networks, malicious node

1. Introduction

We can get extensive information ranging from the physical world to the digital world using wireless sensor networks (WSNs) that consist of a wide range of multipurpose sensor nodes. Each member of the sensor network has the capacity of sensing, signal processing, and wireless communication [1].

One important class of wireless sensor networks is the wireless ad hoc sensor networks, which are characterized by an ad hoc or random deployment sensor method, by which the sensor location and distances among them were not previously known [2].

Due to the limitations of power, sensing, computation, storage, processing, wireless communication capabilities, and especially battery capacities, the current security mechanisms of wired sensor networks or wireless networks cannot be applied directly to WSNs. For this reason, there is a need to develop new techniques or modify the current security mechanisms in order to transfer data reliably from the source node to the sink over intermediate relay nodes [3,4]. Many routing protocols have been proposed for ad hoc and sensor networks. Most of them accept that the intermediate nodes are reliable and thus do not consider the security and/or attack problems. However, this argument may not apply in some cases. For example, in a network environment, some behaviors of malicious nodes can result in not only false alarms but also the exhaustion of the finite amount of energy in a battery. A compromised node can be used to inject fake sensing reports in the sensor area [5]. If

*Correspondence: z.pala@alparslan.edu.tr

not disabled, these fake reports will be forwarded to the base station. In this case, the data sent to the base station will not be realistic.

Can we disable the nodes in the network environment that behave suspiciously from time to time? How will the remaining nodes be affected when this type of node is considered unsafe and thus completely disabled? How will the existent network be affected when suspicious nodes are used as relay nodes or completely disabled? We have created a model using linear programming (LP) to find the answers to these questions.

The rest of our paper is organized as follows. Section 2 reviews the related work. Security assumptions, the threat model, and the system model are presented in Section 3. Analyses based on LP models are presented in Section 4. We conclude the paper in Section 5.

2. Related work

Since the literature on mathematical programming-based optimization, modeling, and analysis of WSNs is extensive and has grown rapidly in recent years [1,6–11], we used LP to construct our framework. Recently, reducing node energy consumption and maximizing lifetime have been studied as important problems [1,6–11]. Some studies have been done on suspicious acting nodes in a network environment. In a network environment some sensor nodes can act suspiciously [12,13] when they enter someone else's control, or due to different device problems [14]. They can drop important data that they have collected [15]. We took necessary measures in our model in order to avoid the loss of important data at suspicious nodes and to rule out suspicious nodes in a network environment. In the literature, most of the studies have been about the detection of suspicious nodes. In [16–18] researchers were primarily concerned with identifying suspicious nodes. In [19], Curiac et al. proposed detecting a malicious node by comparing its output with its estimated value computed by an autoregressive predictor. In [20], Du et al. proposed a scheme to detect malicious attacks in localizations. In [21] Agrawal and Mishra proposed a round time trip (RTT) estimator based on a wormhole detection mechanism to identify wormhole tunneling attacks in mobile ad hoc sensor networks. In [22], Wu proposed a simple authentication protocol for wireless sensor networks based on distributed clustering and asymmetric cryptographic algorithms. In [23], Cui and Yang developed a novel reactive routing scheme that bypassed suspicious nodes by estimating parent nodes' reliability and link quality in an integrated manner.

In this study, we investigate the impact of disabling suspicious nodes communications on network lifetime through an LP framework. We deal with the problem of disabling some sensor nodes in a wireless sensor network to control the possibility of unauthorized access. To the best of our knowledge, there is no previous study that investigated the impact of disabling suspicious nodes' communications on network lifetime in WSNs within an LP framework. The most crucial point of this study is to draw the attention of researchers to security.

3. Concept and model

Our goal in this study was to investigate the maximum achievable sensor network lifetime with different strategies and in different deployment scenarios. In this section we first present the security assumptions and threat model, and then we formulate the system model with an optimization objective function and a set of problem constraints.

3.1. Security assumptions and threat model

In our model, we consider a WSN consisting of a lot of sensor nodes and a base station distributed over an operation area. Each sensor in the network is located independently from the others, and the location of each

sensor node is chosen by sampling the uniform distribution. Sensor nodes generate data that must be sent to the base station, possibly by using other nodes as relays. We accept that all the sensor nodes have the same transmission distance. Sensor nodes can be randomly [24] dispersed or placed in predetermined locations. Nodes with faulty sensors or malicious behavior are identified. A sensor in the network can sense any activity in its communicating range and can communicate with other sensors that lie within its sensing range. We assume that the base station is physically well protected, cannot be easily settled on [25], and is centrally located within the sensing range of each sensor in the sensor field.

Sensor nodes that generate incorrect sensing data or behave maliciously in communication intermittently are treated as unusable nodes. Which sensor nodes are malicious is known. Sensor nodes are deployed in an unattended environment and do not include strong tamper resistance hardware; hence, they are vulnerable to node compromise [26]. A small number of faulty or suspicious sensors [27,28] should not bring down the whole network.

We accept that the number of suspicious node does not change during a simulation or at each l round of simulation. Data are not sent to suspicious nodes, and also data are not accepted from them during the simulation. Thus, the optimization problem is solved without the suspect nodes and the impact of the situation in which suspect nodes are not in communication is investigated on network lifetime. At each l round of the simulation, a source node is selected at random and the generated data packets are sent to the base station at a steady speed from the source node using intermediate nodes. As a result, there is only a single lifetime value in each simulation. This value is the least life duration of a living node [8].

Within this threat model, the security goal is to disable suspicious nodes and reveal the impact of suspicious nodes on the WSN lifetime.

3.2. System model

The ad hoc WSN model used in this application consists of a base station at the center and N_V sensing nodes. The N_0 node is accepted as a base station during the simulation. When a simulation is in the l round, one of the nodes outside the base station performs randomly as the source node and sends a message to the base station during t lifetime extension via nodes between them. For the current model the network topology is represented by a directed graph G = (U, A). U is a node set that includes the base station as N_0. V is the set of nodes excluding base station and S is the set of spy nodes.

A = {(l, i, j): l ∈ L, i ∈ V, j ∈ U-i}is the set of arcs that implies that no node sends data to itself. All messages that will be sent from N_i to N_j during the network lifetime are referred as f_{ij}. All system variables with their acronyms and descriptions that are used in this study are presented in Table 1. The optimization problem of this model is formulated as a LP problem, presented in Figure 1.

As seen in Figure 1, the first constraint of the problem states that all flows in the network are positive (f_{ij}^{l} indicates the direct flow from node N_i to node N_j at round l).

Eq. (2) is used to set flows that do not exist in the model: there cannot be a flow from the base station to another node or from a node to itself.

Eq. (3) states that there cannot be a flow from a malicious node to another node.

Eq. (4) indicates that the difference between the data flowing out of node N_i and the data flowing into node N_i is the data generated at node N_i. This should hold for all source nodes, except the base station and malicious nodes.

Table 1. Terminology for LP formulations.

Variable	Description
G (U, A)	Directed graph representing the network topology
U	The set of nodes including the base station (BS)
V	The set of nodes excluding the base station
S	Set of spy nodes
L	Number of rounds
l	Round of simulation
A	Set of arcs
D_i	Data generated at $N_i$node
N_V	Number of nodes
N_i, N_j	Any node pair in a network environment
N_0	Base station
N_{src}	Source node
K_S	Number of spy nodes
A_V	Deployment area
ρ	The energy consumed in the electronic circuit
α	Transmission path loss exponent
e_i	Energy stored at each sensor node
ξ	Battery energy
f_{ij}	Flow from N_i to N_j
P_{rx}	The amount of consumed energy while receiving one bit of data
$P_{tx,ij}$	The amount of consumed energy while transmitting one bit of data node Ni to node Nj
d_{ij}	The distance between two nodes (node N_i to node N_j)
R_M	Maximum mobility range at each round

Eq. (5) states that f_{flows} can terminate at the base station or at a source node or at a malicious node, but another node should relay f_{flows}.

Eq. (6) states that flows can terminate at the base station or at the source node but another node should relay f_{flows}.

Eq. (7) indicates that for all nodes in the network, except the base station and a malicious node, the energy consumed for transmission and receiving is equal to or less than the energy stored in its batteries. In this study, we neglect the energy spent for sensing, which is minor compared to energy spent for communication [8].

Eq. (8) indicates that for all nodes except the base station the energy consumed for transmission and receiving is equal to or less than the energy stored in batteries.

Throughout this study, we use the energy parameters given in [8]. $P_{tx,ij=}\rho + \varepsilon\ d_{ij}^{\alpha}$ and

$P_{rx} = \rho$ represent the amount of energy for transmission and reception of a bit, respectively. Where ρ models the energy dissipation on electronic circuitry ($\rho = 50$ nJ/bit), ε denotes the transmitter's efficiency ($\varepsilon = 100$ pJ/bit/m^2), α represents the path loss, and d_{ij} is the distance between N_i and N_j.

Eq. (9) indicates that for all nodes except the base station the battery energy is the same.

In this study we have constructed two different models: one is used for a secure situation and the other is used for a nonsecure situation. In Figure 1, Eq. (1), Eq. (2), Eq. (3), Eq. (4), Eq. (5), Eq. (7), and Eq. (9) are used for constraints for our first linear program in the nonsecure model. For the secure model we construct a second model with Eq. (1), Eq. (2), Eq. (3), Eq. (4), Eq. (6), Eq. (8), and Eq. (9) used as the constraints.

$$Maximize \sum_{i \in V} D_i t$$

Subject to:

$$f_{ij}^{l} \geq 0 \; \forall (i,j) \in U, \forall l \in L \tag{1}$$

$$f_{ij}^{l} = 0 \;\; if \; N_i = N_0 \; or \; N_i = N_j \; \forall (i,j) \in A, l \in L \tag{2}$$

$$f_{ij}^{l} = 0 \; if \;\; \forall i \in S \tag{3}$$

$$\sum_{\substack{j \in (U-S) \\ j \neq i}} f_{ij}^{l} - \sum_{\substack{j \in (V-S) \\ j \neq i}} f_{ji}^{l} = D_i^l t \;\; \forall i \in (N_V - K_S) \tag{4}$$

$$\sum_{j \in (U-S)} f_{ij}^{l} = \sum_{j \in (V-S)} f_{ji}^{l} \;\; \forall i \in (N_V - K_S) \; and \; N_i \neq N_{src} \tag{5}$$

$$\sum_{j \in U} f_{ij}^{l} = \sum_{j \in V} f_{ji}^{l} \;\; \forall i \in V \; and \; N_i \neq N_{src} \; \forall l \in L \tag{6}$$

$$P_{rx} \sum_{\substack{l \in L \\ j \neq i}} \sum_{\substack{j \in (V-S) \\ j \neq i}} f_{ji}^{l} + \sum_{l \in L} \sum_{j \in (U-S)} P_{tx} f_{ij}^{l} \leq e_i \; \forall i \in (N_V - K_S) \tag{7}$$

$$P_{rx} \sum_{l \in L} \sum_{\substack{j \in V \\ j \neq i}} f_{ji}^{l} + \sum_{l \in L} \sum_{\substack{j \in U \\ j \neq i}} P_{tx} f_{ij}^{l} \leq e_i \; \forall i \in V, \forall l \in L \tag{8}$$

$$e_i = \xi \;\; \forall i \in V \tag{9}$$

Figure 1. Basic LP framework.

In order to explain the problem we investigate in this study and how our model works in the simplest terms, we made use of linear topology, which is illustrated in its simplest form in Figures 2a–2d.

The 5 nodes on the far left applied in topology were used as base stations and a distance of 100 m was left between nodes. We operated the simulation in 2 different situations, using parameter values in Table 2.

Table 2. List of parameters used in toy example.

Parameters	Values
Deployment scenario	Linear (1-D) equidistant
Model	Stationary
Number of sensor nodes (N_V)	5
Number of round (L)	2
Inter-node distance	100 m
Number of suspicious nodes (K_S)	1
Source node selection	Random
Source node selection domain	(N_V – K_S)
Source node data rate	1 bps
ρ	50 nJ/bit
ε	100 pJ/bit/m^2
α	2

In the first situation, all nodes in the field were accepted as secure. After the simulation had started, the N_4 node (Figure 2a) in the l_1 round and N_1 node (Figure 2b) in the l_2 round were randomly chosen as source nodes, respectively. At each round data were created in 1 bps by means of source nodes, and they were sent via nodes between them. After the simulation came to an end, the lowest network lifetime was calculated as 579,421.564 s.

In the second situation, the nearest node to the base station was accepted as suspicious during the simulation. No message was sent during communication. After the simulation had started, N_4 node (Figure 2c) in the l_1 round and N_2 node (Figure 2d) in the l_2 round were chosen randomly and respectively as the source nodes. At each round data were created in 1 bps by means of source nodes and they were sent via nodes between them. After the simulation came to an end, the lowest network lifetime was calculated as 201,700.642 s. This result is also the total of bits that were sent to the base station from the N_2 source mode.

4. Analysis

In this paper, we used the general algebraic modeling system (GAMS) [29] as a high-level modeling system for mathematical programming and optimization to solve the optimization problem. For a comprehensive analysis of the problem at hand, we solved several instances of the same optimization problem by changing the design parameters.

In the first phase 4 analyses were made for the stationary situation. In one of them, nodes were put into the field using random deployment topology. In the other analyses, as shown in Figure 3, nodes were placed into the area at an accurate and equal distance (the distance between each node is 40 m).

In the first phase of the first analysis, the stationary situation of the nodes that were randomly deployed was analyzed. Locations of nodes in each round were kept constant during the simulation. The effect of spy nodes, which were already known and stable, on network lifetime was analyzed. By dividing the values that changed according to spy nodes in an insecure situation into a reference value taken from when there were no spy nodes, or in other words when there was a completely secure situation, the normalized rate was found. This analysis was done 100 times for each different value of the spy nodes.

In the first phase of the second analysis, 101 nodes were put at a distance of 40 m from each other in a 400 m $\times$ 400 m area (Figure 3). The N_0 node was always at the center as a base station. As shown in Figures 4a–4d respectively, spy nodes were increased by including (x, y), (–x, y), (–x, –y), and (x, –y) coordinate systems in $10S_K$ numbers and thus the effect of the increase on network lifetime was investigated. This analysis was done 100 times for each different value of spy nodes.

In the first phase of the third analysis, 101 nodes were put at a distance of 40 m from each other in a 400 m $\times$ 400 m area. As shown in Figures 5a–5d, the number of spy nodes was increased from the exterior part to the interior on the condition that they would focus around the base station, and the effect of the increase on network lifetime was analyzed. This analysis was done 100 times for each different value of spy nodes.

In the first phase of the fourth analysis, 101 nodes were put at a distance of 40 m from each other in a 400 m $\times$ 400 m area. As shown in Figures 6a–6d the number of spy nodes was increased from the interior part to the exterior and the effect of the increase on network lifetime was analyzed. This analysis was done 100 times for each different value of spy nodes.

In the second phase, the analysis was done using a random deployment model. Having operated a random deployment model, the transmission of messages via changing topology in each l round was analyzed to find out if they were secure (when there were no spy nodes) or insecure (when there were spy nodes). This analysis was done 100 times for each different value of spy nodes.

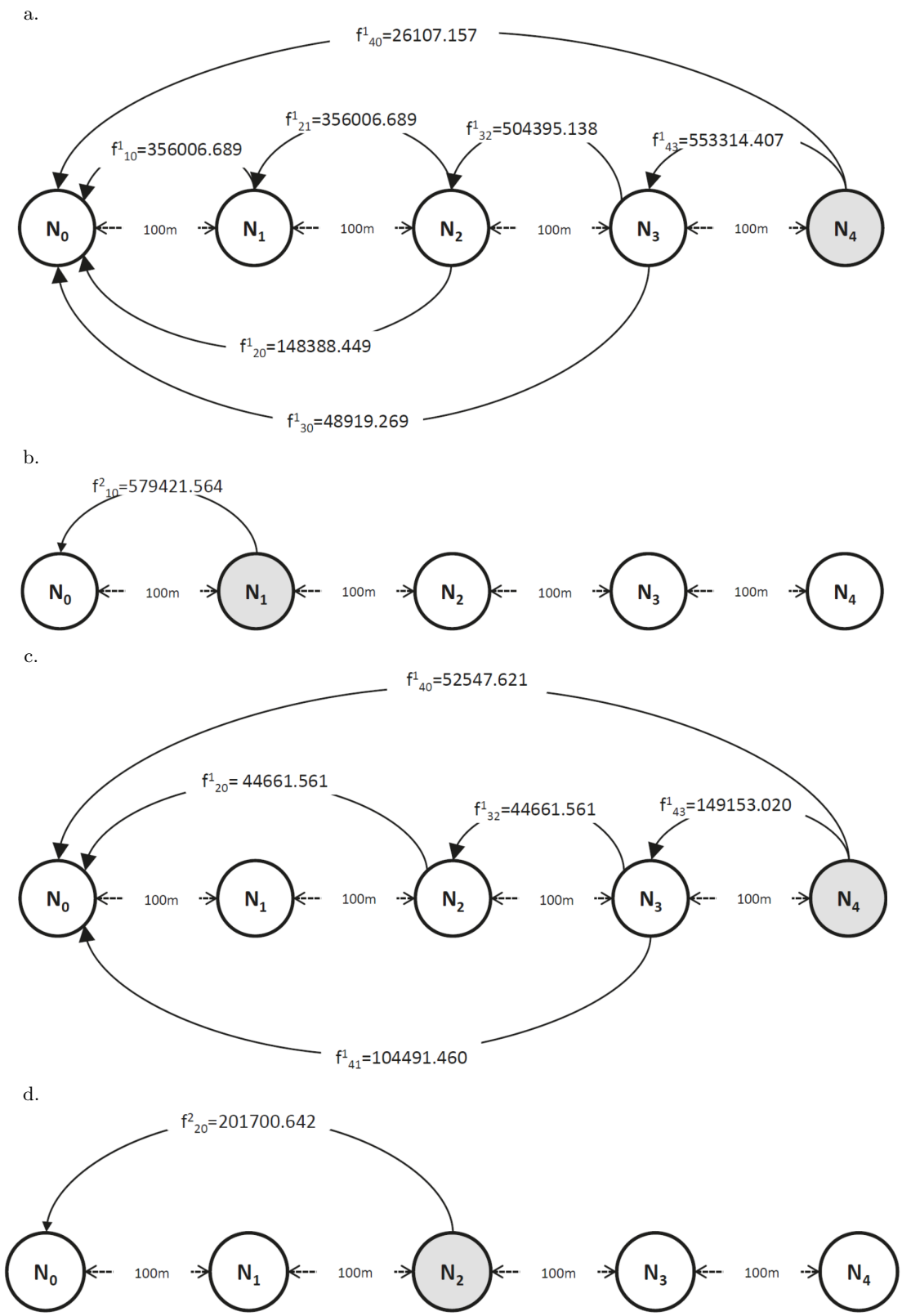

Figure 2. All nodes in the field were accepted as secure. a. All nodes in the field were accepted as secure and N_4 node is source node in l_1 round. b. All nodes in the field were accepted as secure and N_1 node is source node in l_2 round. c. In insecure mode N_4 node is source node in l_1 round. d. In insecure mode N_2 node is source node in l_2 round.

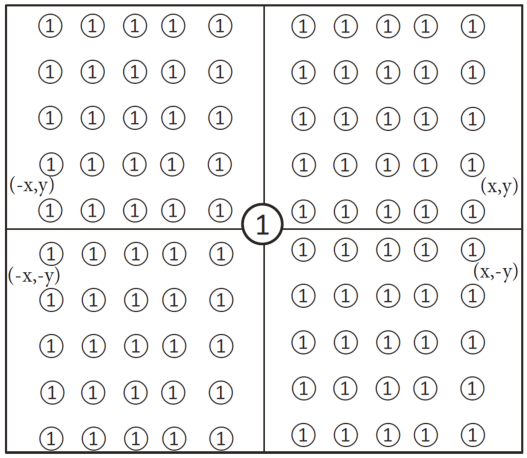

Figure 3. A total of 101 sensors are deployed in the sensor field equally spaced. The distance between two sensors is 40 m. A base station is centrally located in the field. The white-filled nodes are secure nodes and they are shown with number 1.

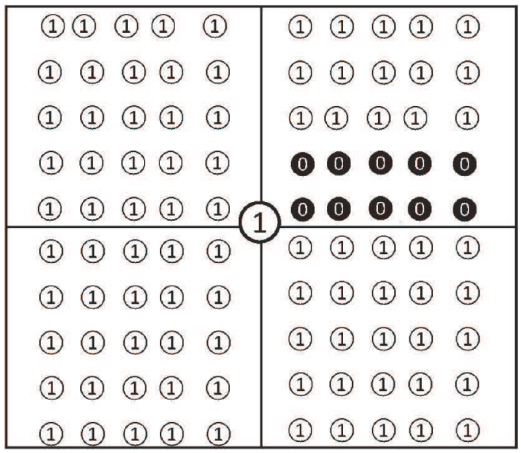

Figure 4 (a). S_K=10.

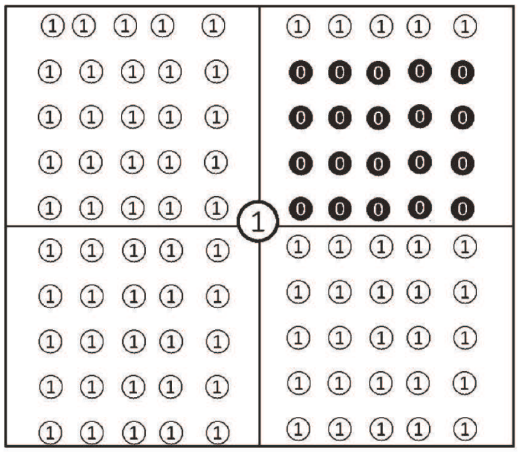

Figure 4 (b). S_K=20.

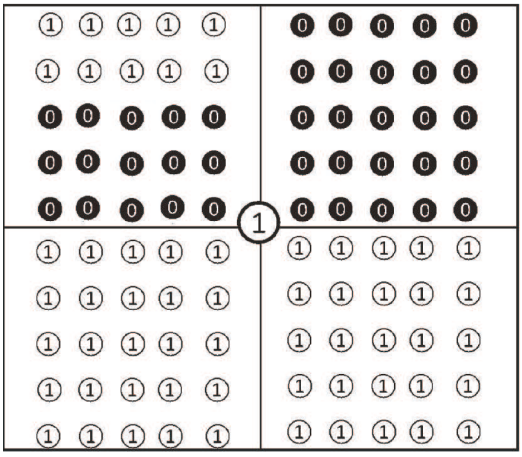

Figure 4 (c). S_K=40.

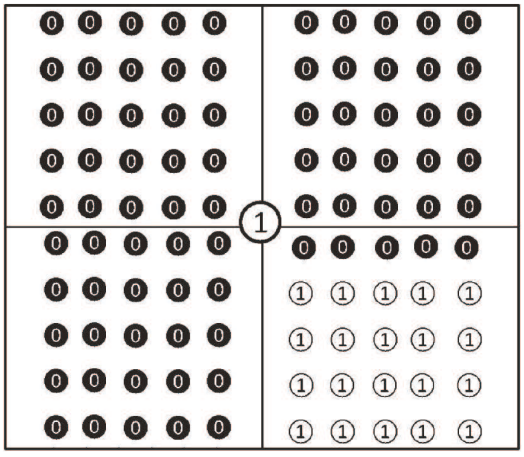

Figure 4 (d). S_K=80.

Figure 4. The black-filled nodes are malicious nodes and they are shown with 0. Packets transferred through these nodes will be dropped randomly or not forwarded as desired. The number of malicious sensors is increased over time. The percentages of the suspicious nodes are: (a) 10%, 4 (b) 20%, (c) 40%, and (d) 80%.

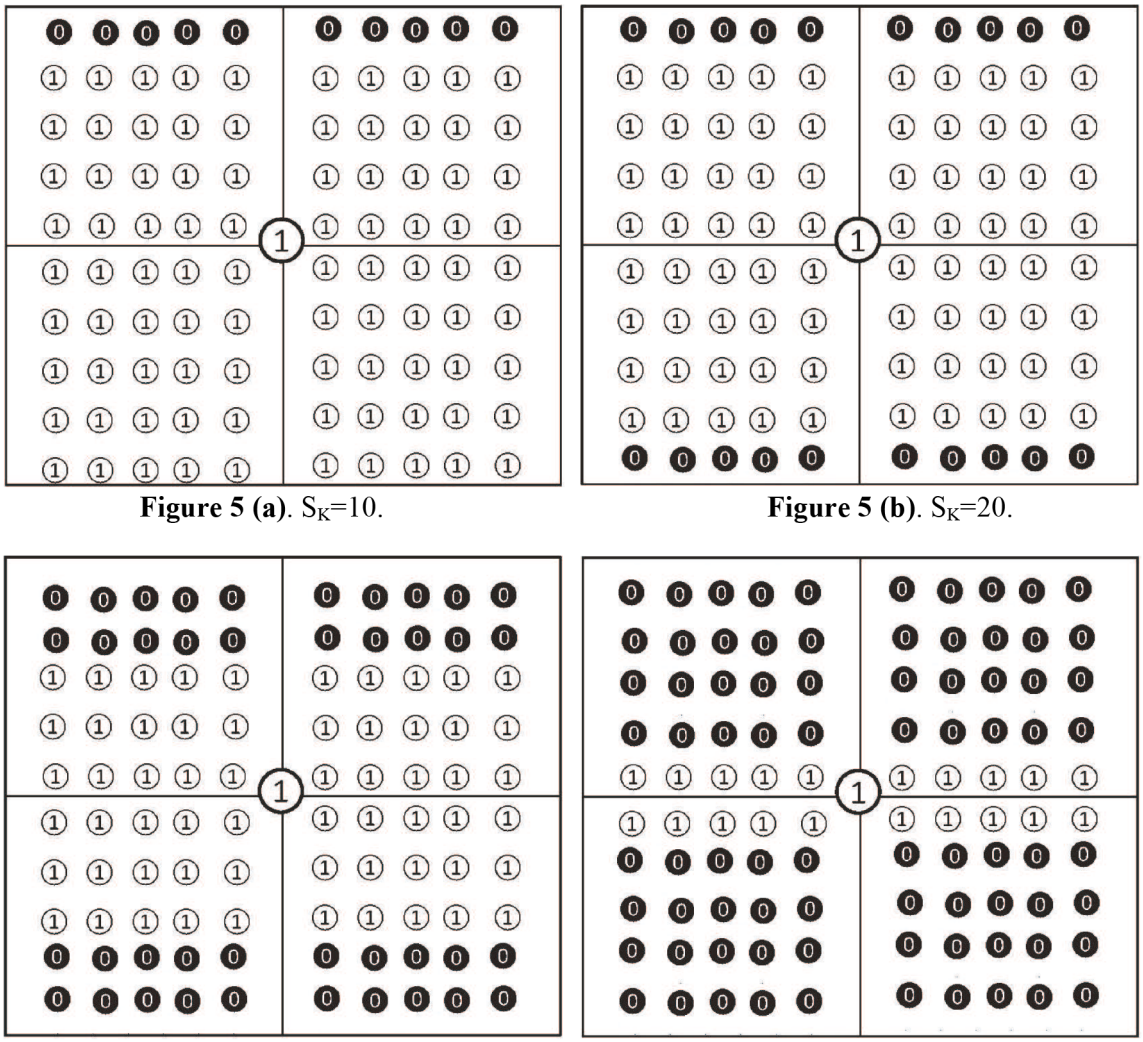

Figure 5 (a). S_K=10. **Figure 5 (b)**. S_K=20.

Figure 5 (c). S_K=40. **Figure 5 (d).** S_K=80.

Figure 5. Increasing of the suspicious sensor nodes from the outside to inside. The percentages of the suspicious nodes are: (a) 10%, (b) 20%, (c) 40%, and (d) 80%.

4.1. General principles of the stationary model

In the model, 101 nodes were used, one of which was the base station, deployed in a square area. At the beginning of the simulation, all nodes are randomly placed in the area in a random deployment model or uniformly deployed in uniform model. Therefore, the spy nodes are also randomly or uniformly placed. All the nodes in the model are motionless. This motionless state never changes during all l rounds of a simulation. Therefore, the spaces between nodes also do not change.

The source node that will produce data in each running of the model and in l round of each running randomly changes. The source node is chosen among (N_V − K_S) nodes, i.e. from among all nodes apart from spy ones. Data are sent by only the source node in each l round of the simulation and the middle nodes reach the base station through nodes. Generation of speed in bits per second of the source node for each l round was fixed at 1 bps. It was accepted that in a simulation, each node, apart from the base station, has 1 J of energy (e_i = 1 J,∀i ∈ V). Only one lifetime value is obtained after the optimization problem has been solved for all l

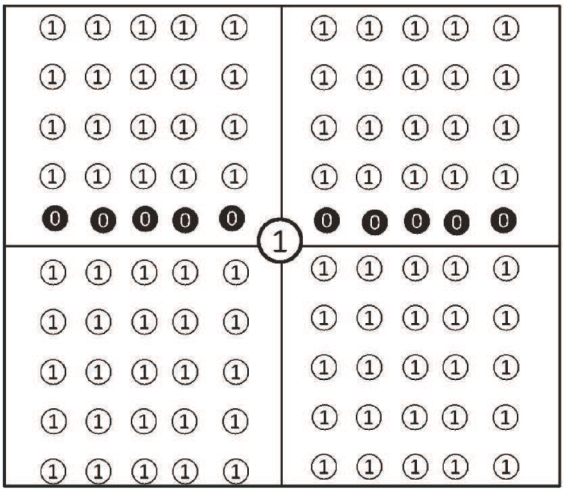

Figure 6 (a). S_K=10.

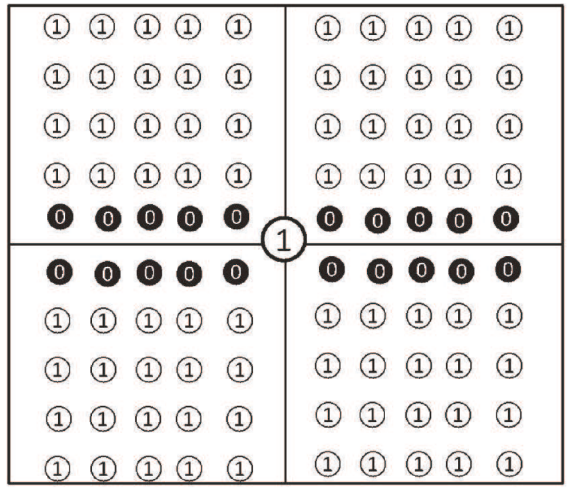

Figure 6 (b). S_K=20.

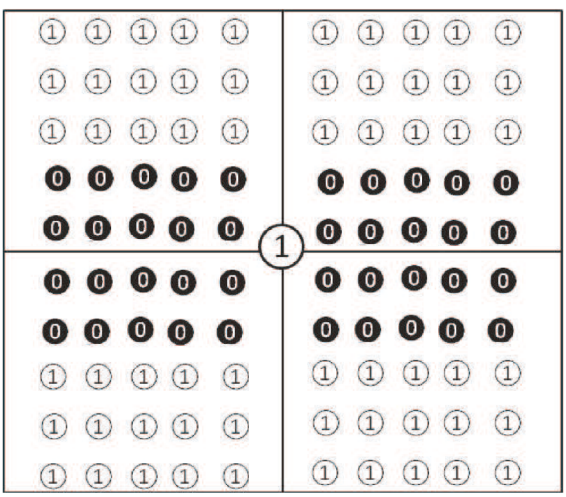

Figure 6 (c). S_K=40.

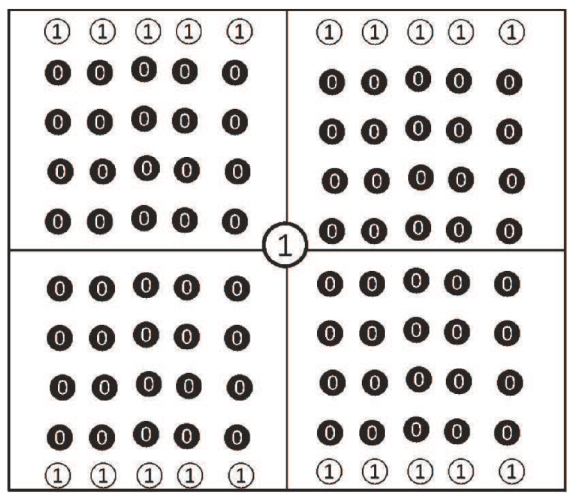

Figure 6 (d). S_K=80.

Figure 6. Increasing of the suspicious sensors from the inside to outside. The percentages of the suspicious nodes are: (a) 10%, (b) 20%, (c) 40%, and (d) 80%.

rounds until it reaches the L round number. This lifetime is the lifetime of the least-longest living node [8].

In the first stage, the simulation was operated for 100 times according to the values in Table 3 and by fixing the parameters in the model. This operation also meant that there were no spy nodes and all nodes were in a reliable condition. The average of these obtained values was used as the reference value in normalization.

In the second stage, the spy node number was fixed between ($K_{init} - K_{finally}$) and this state was changed for all the rounds of a simulation. The parameter values in Table 3 were used for the simulation and the simulation was operated 100 times.

In the third and following stages, the spy node number was increased up to 5 and each simulation was operated 100 times. The average value was obtained for the situation in which each spy node number was used. For the values of spy node numbers between 5 and 80, the average of each 100 operations was calculated. It was divided into the state in which the spy node number was 0 at the beginning, and normalized lifetime values were obtained.

Table 3. List of used parameters in analysis without mobility

Parameters	Values
Model	Stationary, random deployment, stationary (in to out/out to in, stationary from 1st region to 4th region)
Deployment scenario	Square topology (2-D)
Node deployment	Initially random/random/equally spaced
Network area (A_V)	400 m × 400 m
Number of sensor nodes (N_V)	100
Number of round (L)	50
Model number of execution	100
The base station location	Centrally located
Number of suspicious nodes (K_S)	0–100
Inter-node distance	40 m
Source node selection	Random
Source node selection domain	(N_V– K_S)
Source node data rate	1 bps
ρ	50 nJ/bit
ε	100 pJ/bit/m^2
α	2

4.2. Analysis results of stationary model

As shown in Figure 7 the existence of spy nodes in a stationary state and the fact that they do not take charge in communications negatively affects the lifetime of nodes. It can be observed that as the number of spy nodes increases, the lifetime of nodes decreases. The main reason for this decrease is that the fixed area that a decreasing number of stable nodes must control becomes too big, and the distance between stable nodes increases. The shortening of lifetimes is sharply seen when the spy node number is 10 or more. In a stationary model if the spy node number is 10, the network life shortens by 12%; if it is 20, the shortening is 24%; and if it is 80 then the network life is shortened by 87%.

As shown in Figure 7 the fact that all nodes are placed in the same conditions, apart from the base station, and at different points in the area during each l round in a random deployment model has enabled them to have a long life according to stationary topology. The ratio in question is not so high, but we can say that this is the result of the instant mobility. In this model, the ongoing increase of spy node numbers resulted in the regular shortening of network life. This decrease is explained by the following.

Sensor nodes in the field decrease over time, but the area itself remains the same. The distance between the sensor nodes in the area will increase. In the random deployment model, if the spy node number is 10, the network life shortens by 11%; if it is 20, the shortening is 21%; and if it is 80 then the network life is shortened by 86%.

In the stationary uniform model, the increasing form of spy nodes in 3 different positions is given comparatively, as shown in Figures 4a–4d, Figures 5a–5d, and Figures 6a–6d, respectively. In the situation in which spy nodes increase from inward to outward (Figure 8), a soft and regular decrease is observed in the lifetime chart. The best lifetime is shorter than the lifetime it shows, because the nodes much nearer to the base stations have much greater burdens. The increase of lifetimes when the spy nodes are in the numbers of 25, 50, and 75, which increase from the first to the fourth region of the coordinate system's left side (Figures 4a–4d), shows that an area has been completely disabled (Figure 8). When the spy node number reaches 25,

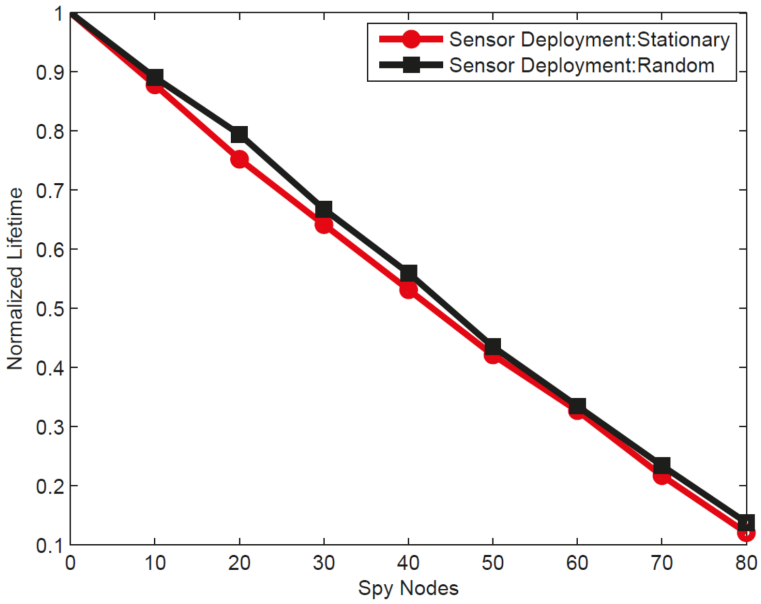

Figure 7. The impact of malicious nodes' increment during stationary and random deployment on network lifetime.

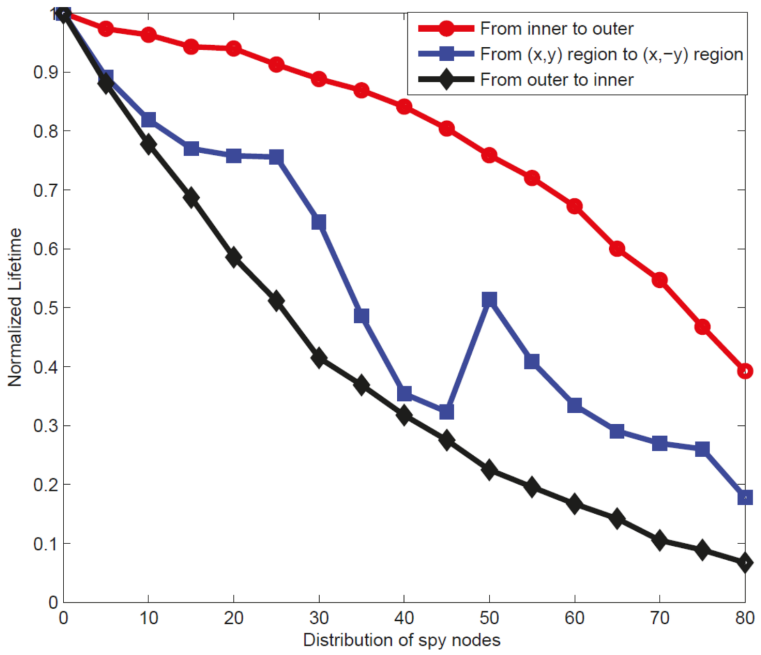

Figure 8. In a stationary uniform model, the increasing form of spy nodes in 3 different positions has been given comparatively.

then the whole of the first coordinate system zone (x, y) is disabled. The instant increase seen here will stop and a decrease will be observed in the following simulations.

A normalization process was also conducted for each situation in which spy node numbers were 10, 20, 40, and 80, respectively. The normalization process was conducted by dividing the results obtained for the values of the R_M mobility radius that were bigger than 0 by the value of the R_M mobility radius that is 0. The spy

node numbers in all changing R_M values were the same for each analysis given in the chart. For example, the spy node number of R_M between 0 and 100 m vfor $S_K = 10$ was fixed.

4.3. Analysis results of the mobility model

In the first analyses, the effect of mobility on lifetime was analyzed considering the number of random spy nodes in an area. This analysis investigated the mobility effect when the spy node numbers were 10, 20, 40, and 80. The radius was enlarged by 10 m for each situation and it was changed between 0 and 100 m. Whenever the mobility radius was changed, the simulation was run 100 times. The position of each node in each l_1 round during simulation changed as did R_M from the previous position (l_0 round).

As shown in Figure 9, we can clearly see the positive effect of mobility on lifetime despite the existence of spy nodes. Mobility has increased the lifetime up to the $R_M = 40$ m value for analyses but it has caused a decrease in the following values [9]. The reason for this is the safe nodes decreasing in number in an area whose size never changes, which means they are controlling an area of the same size with a smaller number of nodes. Nodes having big mobility values change their places in each l round of the simulation up to R_M. The best result among mobility-aided analyses for random deployment was obtained in the case where the spy node number is 10. The results in Figure 9 are the ones obtained in the case where there are no spy nodes. The average results in each curve given in the chart in question are divided into the values in which there are no spy nodes but only mobility. As a result, it is clearly seen that the main factor in increasing lifetime is mobility.

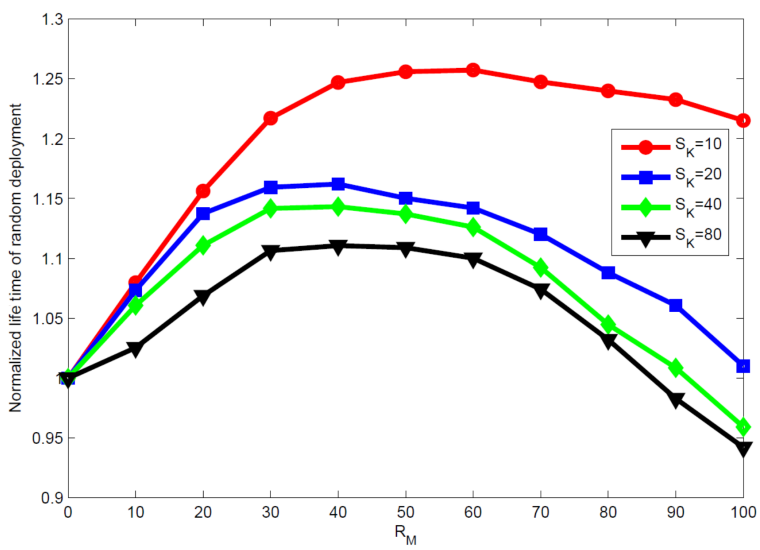

Figure 9. Normalized lifetime change rates in terms of $S_K = 10$, $S_K = 20$, $S_K = 40$, and $S_K = 80$ for the random deployment topology with the mobility radii varied from 10 m to 100 m for 101 sensor nodes.

As shown in Figure 10, 4 different analyses were made in order to observe the increase in spy node from the first coordinate system region (x, y), as indicated in Figures 3 and 4, to the fourth coordinate system region (x, –y), as indicated in Figures 3 and 4. In the analyses in which spy node number is accepted as 10 ($S_K = 10$), mobility increased the lifetime up to $R_M = 40$ m but after this value, it decreased the lifetime. The normalization process was carried out by making no change in the number of spy nodes and according to the situation in which there was no mobility ($R_M = 0$). Therefore, it was expected that lifetime would increase with small mobility values. On the other hand, the same result cannot be obtained with higher mobility values.

In the analyses, the effect of mobility for $S_K = 20$ is felt less. This decrease can be based on the protection of a fixed area with a lower number of nodes. Besides, it is necessary to pay attention to the fact that 80% of nodes in the first coordinate system region (x, y) are accepted as spy nodes. Although the lifetime observed for $S_K = 40$ is higher than the value observed for $S_K = 20$, it does not mean that the former provides a high lifetime. Each chart point has been obtained by dividing that value into the reference value reached for $R_M = 0$, depending on the spy number. The mobility effect observed in each chart is pursuant to their own reference values.

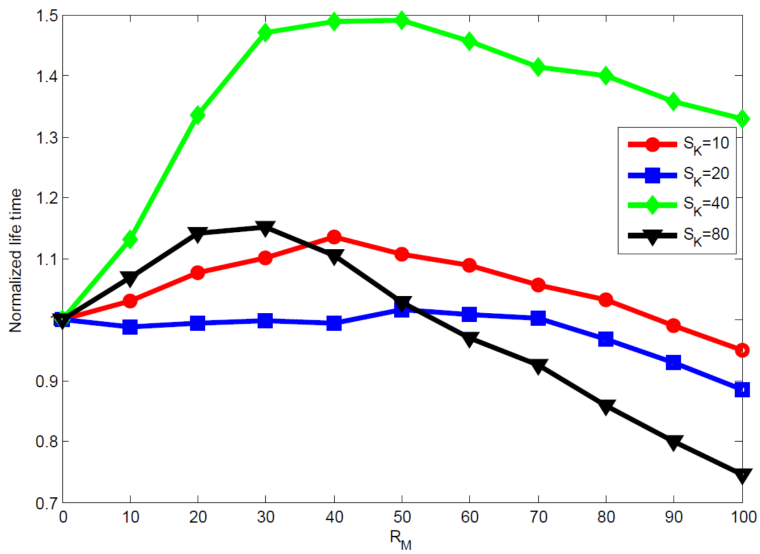

Figure 10. Normalized lifetime change rates in terms of $S_K = 10$, $S_K = 20$, $S_K = 40$, and $S_K = 80$ for the uniform deployment topology with the mobility radii varied from 10 m to 100 m for 101 sensor nodes.

5. Conclusion

The crucial resource in wireless ad hoc sensor networks is energy. For this reason, in this study we analyzed the energy dissipation and network lifetime characteristics of methods for detecting and disabling malicious nodes in wireless ad hoc sensor networks through novel LP formulations.

Our results reveal that the existence of spy nodes in a stationary state and the fact that they do not take charge in communications negatively affects the lifetime of nodes. It has been observed that as the number of spy nodes increases, the lifetime of the nodes decreases. The shortening of lifetimes is sharply seen in values of spy node numbers at 10 or greater. Our results show that the decrease in WSN lifetime is less than 8.0% if the numbers of suspicious node are not higher than 10%.

References

[1] İncebacak D, Bicakci K, Tavli B. Evaluating energy cost of route diversity for security in wireless sensor networks. Comp Stand Inter 2015; 39: 44-57.

[2] Cardei M, Wu J, Lu M, Pervaiz M. Maximum network lifetime in wireless sensor networks with adjustable sensing ranges. In: International Conference on Wireless and Mobile Computing, Networking and Communications; 22–24 August 2005. pp. 438-445.

[3] Reddy YB. A game theory approach to detect malicious nodes in wireless sensor networks. In: International Conference on Sensor Technologies and Applications; 18–23 June 2009; Athens, Greece. pp. 462-468.

[4] Liu CX, Liu Y, Zhang ZH, Cheng ZY. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. Int J Commun Syst 2012; 26: 380-394.

[5] Ye F, Luo H, Luand S, Zhang L. Statistical en-route filtering of injected false data in sensor networks. IEEE J Sel Area Comm 2005; 23: 839-850.

[6] Liu G, Xu B, Chen H. An indicator kriging method for distributed estimation in wireless sensor networks. Int J Comm Syst 2014; 27: 68-80.

[7] Batmaz AU, Yildiz HU, Tavli B. DDRP: Role of unidirectionality and reverse path length on wireless sensor network lifetime. IEEE Sens J 2014; 14: 3971-3982.

[8] Cheng Z, Perillo M, Heinzelman W. General network lifetime and cost models for evaluating sensor network deployment strategies. IEEE T Mobile Comput 2008; 7: 484-497.

[9] Pala Z, Bicakci K, Turk M. Effects of node mobility on energy balancing in wireless networks. Comput Electr Eng 2015; 41: 314-324.

[10] Pala Z. Effects of mica2-based discrete energy levels on lifetime of cooperation neighbor sensor networks. Turk J Elec Eng & Comp Sci 2016; 24: 2671-2678.

[11] Yuksel A, Uzun E, Tavli B. The impact of elimination of the most critical node on wireless sensor network lifetime. In: IEEE Sensors Applications Symposium; 13–15 April 2015. pp. 1-5.

[12] Rajasegarar S, Leckie C, Palaniswami M. Anomaly detection in wireless sensor networks. IEEE Wirel Commun 2008; 15: 34-40.

[13] Jabeura N, Sahlib N, Khanc IM. Survey on sensor holes: a cause-effect-solution perspective. Procedia Computer Science 2013; 19: 1074-1080.

[14] Zhou Y, Cai X. An approach to detect sensor node anomaly in wireless sensor network. In: Computer Network and Multimedia Technology Symposium; 18–20 January 2009; Wuhan, China. pp. 1-4.

[15] Yu B, Xiao B. Detecting selective forwarding attacks in wireless sensor networks. In: IEEE Parallel and Distributed Processing Symposium; 25–29 April 2006.

[16] Ngai ECH, Liu J, Lyu MR. On the intruder detection for sinkhole attack in wireless sensor networks. In: IEEE International Conference on Communications; June 2006; İstanbul, Turkey. pp. 3383-3389.

[17] Pires WR, de Paula Figueiredo TH, Wong HC, Loureiro AAF. Malicious node detection in wireless sensor networks. In: IEEE Parallel and Distributed Processing Symposium; 26–30 April 2004.

[18] Usman M, Muthukkumarasamy V, Xin-Wen Wu, Khanum S. Wireless smart home sensor networks: mobile agent based anomaly detection. In: Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing; 4–7 September 2012; Fukuoka, Japan. pp. 322-329.

[19] Curiac DI, Banias O, Dragan F, Volosencu C, Dranga O. Malicious node detection in wireless sensor networks using an autoregression technique. In: Third International Conference on Networking and Services; 19–25 June 2007; Athens, Greece. pp. 83-88.

[20] Du W, Fang L, Ning P. LAD: Localization anomaly detection for wireless sensor networks. In: IEEE Parallel and Distributed Processing Symposium; 4–8 April 2005. p. 41a.

[21] Agrawal N, Mishra N. RTT based wormhole detection using NS-3. In: Computational Intelligence and Communication Networks, International Conference; 14–16 November 2014; Bhopal, India. pp. 861-866.

[22] Wu B. A hierarchical authentication scheme in wireless sensor networks. In: Mobile Ad Hoc and Sensor Systems, IEEE 11th International Conference; 28–30 October 2014; Philadelphia, PA, USA. pp. 630-635.

[23] Cui B, Yang SJ. NRE: Suppress selective forwarding attacks in wireless sensor networks. In: Communications and Network Security, IEEE Conference; 29–31 October 2014; San Francisco, CA, USA. pp. 229-237.

[24] Li W. Wireless sensor network placement algorithm. In: International Conference on Wireless Communications, Networking and Mobile Computing; 24–26 September 2009; Beijing, China. pp. 1-4.

[25] Lee SJ, Chun IG, Kim WT, Park SM. Control method for the number of checkpoint nodes for detecting selective forwarding attacks in wireless sensor networks. In: International Conference on Information and Communication Technology; 17–19 November 2010; Jeju, Korea. pp. 537-538.

[26] Newsome J, Shi E, Song D, Perrig A. The Sybil attack in sensor networks: analysis and defenses. In: Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks; 26–27 April 2004. pp. 259-268.

[27] Tahir H, Shah S. Wireless sensor networks-a security perspective. In: Proceedings of the 12th IEEE International Multi-Topic Conference; 23–24 December 2008, Karachi, Pakistan. pp. 189-193.

[28] Saihi M, Boussaid B, Zouinkhi A, Abdelkrim MN. WSN implementation of DFD algorithm on SOFREL S550/WAVENIS unit. In: Sciences and Techniques of Automatic Control and Computer Engineering, 15th International Conference; 21–23 December 2014; Hammamet, Tunisia. pp. 219-224.

[29] Rosenthal RE. GAMS: A User's Guide. Washington, DC, USA: GAMS Development Corporation, 2015.