ISSN: 2458-8989

Natural and Engineering Sciences

NESciences, 2017, 2(3): 45-58

-RESEARCH ARTICLE-

A Centralized Detection Of Sinkhole Attacks Based On Energy Level Of The Nodes On Cluster-Based Wsns

Merve Nilay Aydın[1*], İpek Abasıkeleş Turgut[2]

[1 2] Iskenderun Technical University, Department of Computer Engineering, Hatay, 31200

Abstract

Wireless Sensor Networks (WSNs) consist of thousands of small and low-cost devices, which communicate over wireless medium. Due to locating in harsh environment and having limited resources, WSN is prone to various attacks. One of the most dangerous attacks threatening WSN is the sinkhole attack. In this paper, sinkhole attack is modelled on a cluster-based WSN and a centralized detection algorithm based on the remaining energies of the nodes is proposed. The simulations are run for different values of energy thresholds and various numbers of nodes. The performance of the system is investigated over total energy consumption in the system, the number of packets arrived at base station and true detection rate of the sinkhole node(s). The results show that the proposed method is both energy-efficient and detects the malicious nodes with a 100% accuracy for all number of nodes.

Keywords:
Wireless sensor networks, security, sinkhole, intrusion detection, LEACH

Article history:
Received 29 September 2017, Accepted 29 October 2017, Available online 30 October 2017

Introduction

Wireless sensor networks (WSNs), which consist of thousands of small and low-cost devices using wireless communication, is adaptable to many environments. WSNs have been successfully implemented in various fields such as habitat monitoring, medical and military applications, and earthquake detection and decision support systems. However, sensor nodes, which have limited

[*] *Corresponding Author: Merve Nilay Aydın, email: mnilay.aydin@iste.edu.tr*

resources such as processor, battery and memory, are usually located in difficult conditions like hostile environments. Therefore, the communication between the transmission channel and the sensor nodes is open to attack. Security as well as the proper functioning of these networks is an important issue to be addressed. In many disaster scenarios, especially planned by terrorists, it is necessary to protect the network from unauthorized access. Hence, it is very important to take security precautions against the attacks threatening the applications of WSNs (Butun, I et al., 2014).

The attacks can be divided into two categories, including insider and outsider attacks. In outsider attacks, attackers organize attacks to disrupt the function of target WSNs by their own nodes without having the necessary secret keys of the network. Thus, outsider attacks can be detected by switching, encryption/decryption and/or authentication methodologies. However, in insider attacks, the attacker can export the information of the network and/or cause the entire network to be compromised by capturing legal system node(s) (Gondwal, N., & Diwaker, C. 2013).

There are different types of insider attacks including sinkhole, black hole, wormhole, flooding and selective forwarding. Sinkhole is one of the most dangerous insider attack, in which a malicious node tries to infiltrate the network, either by forcing a sensor node into danger or using another malicious node in the network to launch an attack (Xing, K et al., 2010). Sinkhole nodes try to deceive the system nodes by announcing that the shortest path from the node to BS cross through themselves. After obtaining the information of the traffic of the network and leading up the nodes to send their packets to themselves, the attackers can harm the network by not sending, copying or flooding the packets (Chaudhry, J. A et al., 2013). The behaviour of a sinkhole attack varies according to the routing architecture of WSN. In flat WSNs, the role of the sinkhole attack is the same for every node, while in a cluster-based WSN, the attacker can be a cluster head or a member node, which results in different levels of injury.

Detecting sinkhole attacks in WSNs is an attractive topic in literature. Some of the studies use cryptographic methods (Sharmila, S., & Umamaheswari, G., 2011; Papadimitriou, A et al., 2009; Bahekmat, M et.al., 2012), while the others suggest non-cryptographic solutions (Han, G et al., 2014; Ngai, E et al., 2007; Radhikabaskar, D et.al, 2014; Chen, C et al., 2010; Patil, S. S., & Khanagoudar, P. S. 2012; Singh, S. K et al.,2011). Cryptographic methodologies are based on the principle of authentication with the use of various keys. On the other hand, non-cryptographic solutions usually benefit from analysing the behaviour of the network for detecting malicious activities. Generally, a centralized authority, which is considered to be trusted and has no resource constraints like WSN nodes, i.e. base station (BS), takes on this task. Non-cryptographic studies propose different technics to detect malicious nodes including neighbour node information (Han, G et al., 2014), packet flow path (Ngai, E. C et al., 2007), network traffic (Radhikabaskar, D. P et al, 2014), CPU usage of nodes (Chen, C et al, 2010), port number, IP addresses (Patil, S. S., & Khanagoudar, P. S., 2012) and MAC addresses of the nodes (Singh, S. K et al., 2011). In this study, sinkhole attack is modelled on a cluster-based WSN architecture and differently from the previous studies in literature, a centralized detection mechanism based on the remaining energy level of the nodes is proposed. Detailed simulations are conducted for various number of nodes and different values of energy thresholds.

Materials and Methods

Simulation Environment

In this study, sinkhole attacks are modelled by simulation with using OMNeT ++ (Varga, A., 2010) on a clustered-based network architecture. LEACH (Heinzelman, W. R et al., 2000) protocol, which is one of the most common hierarchical routing protocol in WSNs, is used. Figure 1 shows a cluster-based WSN architecture. Three main components are included in the system: BS, cluster head (CH), and member node (MN). BS is responsible for evaluating the data collected from the CHs, while CHs collect data from their MNs. The sensing data originates from MNs. Each MN is a member of cluster with a unique CH.

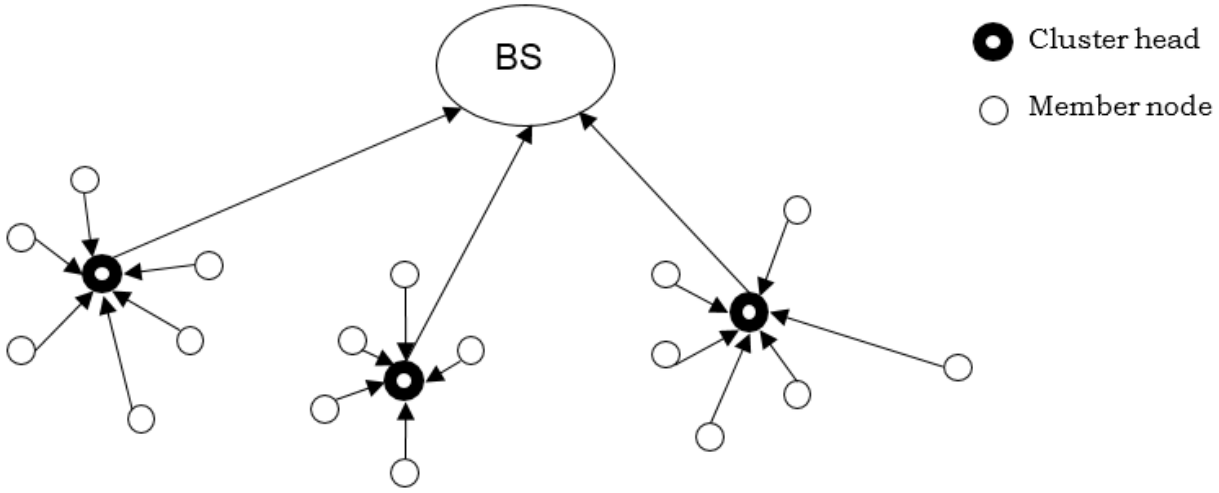

Figure 1. A cluster-based WSN architecture.

Sinkhole attacks can be modelled in various forms on WSNs. However, how these attacks are modelled plays a crucial role on performance of the system. In this study, 10% of total numbers of the nodes in the network is added to the network as a malicious node and the damage of these nodes to the network is investigated by tracing packet transmission. As the **proposed network architecture** is a cluster-based topology, the role of the malicious node varies according to its level in hierarchy. As is seen in **Figure 2 and Figure 3**, if the malicious node is a MN, it damages the **proposed network** by not forwarding its sensed data to CH. However, if the role of the malicious node is a CH, then the aggregated data collected from all of the cluster MNs is not transmitted to BS, which causes much more damage to the network.

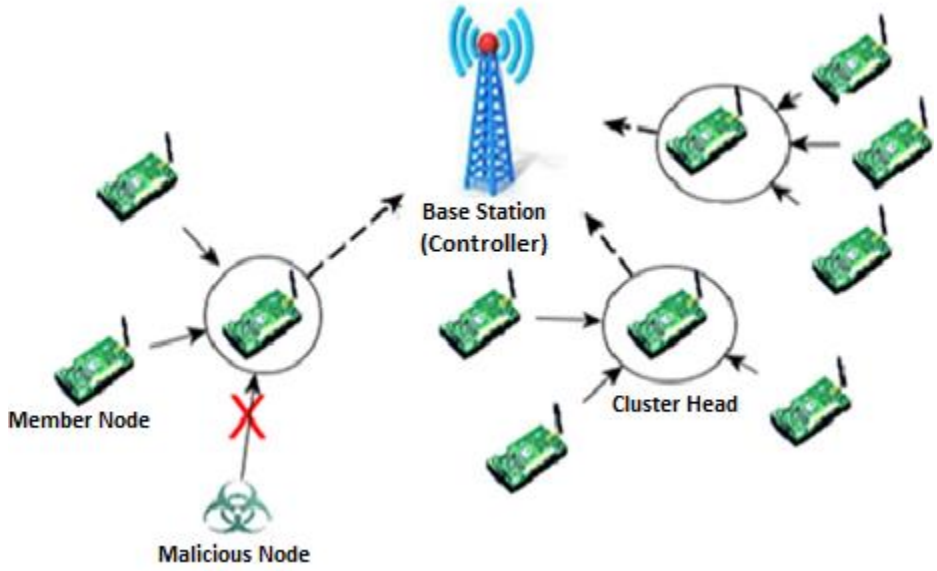

Figure 2. Sinkhole node as a MN.

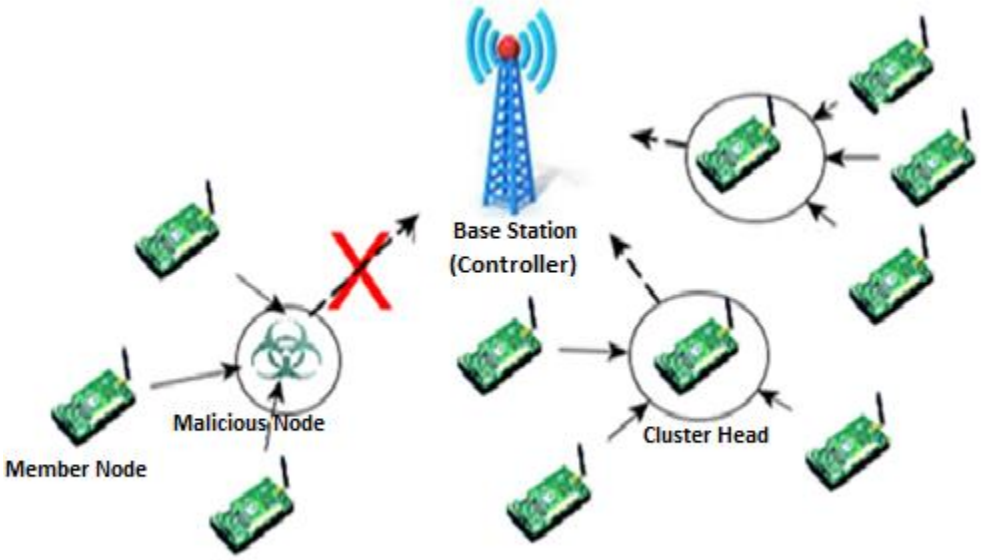

Figure 3. Sinkhole node as a CH.

Detection of Sinkhole Attacks

The **proposed detection mechanism** consists of two stages. The list of the suspect nodes is created in the first stage, while the second stage is responsible for determining if a node is malicious or not. These operations are conducted by a centralized authority, i.e. BS, which is considered to have enough resources and to be trustworthy. Initially, BS compares the packets received in the last round with that of previous round. If a node have not sent a packet in the current round, but have sent in previous one, then it is added to suspicious (potentially malicious)

list. In the second stage, BS controls the remaining energy level of the suspicious nodes. If battery level of a suspect node is below a certain threshold value, then the node is considered to be dead and no further action is taken. However, if remaining energy of a suspicious node is above this value, BS requests the data of the node by sending a query message and waits for response. If the node does not respond to query, BS labels the node as malicious.

Choosing an optimum threshold value is crucial with regards to the performance of the proposed detection methodology. If the threshold value is too low, BS sends a large number of query messages, which in turn causes extra energy consumption in the system. If a high threshold value is chosen, it will be difficult to identify malicious nodes because a few query messages will be sent to suspect nodes. When BS detects a malicious behaviour in the system, it sends an ALARM message including the identity information of the malicious node(s) to the other nodes in the network as a response action. When system nodes take the ALARM message, they break their link with the malicious node(s). Hence, the system is considered to sweep the sinkhole attack away. If BS does not detect any harmful behaviour for current round, then it sends CONTINUE message to the nodes in order to start the next round. It is assumed that these is not any malicious node in the system in the first round.

The Messages of the System

There are two types of messages produced by the system. The first one is the messages originated from the LEACH protocol and the second one is the additional messages created by the proposed algorithm in order to identify the malicious nodes in the system.

As is seen in Table 1, there are four types of messages created by LEACH protocol. The size of the packets carrying data is considered to be four times of the size of the broadcast and control messages in the system.

Table 1. The messages of LEACH Protocol

Name	Explanation	Function	Size
ADV	Advertisement Message	For announcement of CHs	
ADV_RES	Response to Advertisement Message	Connection request from MNs to CHs	
DATA_MN	Data Message	Data Message from MNs to CHs	X
DATA_CH	Data Message	Aggregated Data Message from CHs to BS	X

ADV message is broadcasted by CHs to the network in order to announce the MNs about their identities and locations. When MNs get ADV messages, they calculate their distance to each CH, choose the closest one as their CH and send ADV_RES message to selected CH for participating in its cluster. After this stage, the clusters are formed and data transition can be started. Initially, MNs send their sensed data to corresponding CH in DATA_MN messages. When CHs collects all data from their cluster, they implements aggregation function and send the produced data in DATA_CH message to BS.

Table 2 shows the messages generated by the proposed detection methodology. When BS suspects about a sinkhole attack after comparing the energy level of the suspicious node, it sends a QUERY message to suspicious node and asks to send its data again. If the node is not a sinkhole node, then it replies the QUERY message with Q_RES message including its sensed

/aggregated data according to its role. If BS does not take a Q_RES message, it labels the node as a sinkhole node and broadcasts an ALARM message to the network including the identity of the sinkhole node. Otherwise, BS creates and broadcasts a CONTUNIE message to start the next round. QUERY, ALARM and CONTUNIE messages are control messages and the size of these messages are equal to that of LEACH control messages. However, the size of Q_RES is four times of the size of the other messages due to carrying data.

Table 2. The messages of sinkhole detection algorithm

Name	Explanation	Function	Size
QUERY	Query Message	BS asks the suspicious node to send its data again	
Q_RES	Reply Message to Query Message	Suspicious node sends its data to BS after taking QUERY message	X
ALARM	Alarm the system	Created by BS to report the sinkhole nodes to the network	
CONTUNIE	Continue to Next Round	Created by BS to start the next round	

Simulation Parameters

Table 3 shows the simulation parameters used in the system. BS is located at the centre of a 1000m x 1000m network.

As seen in the table, a 50, 100, 150, and 200 nodes are randomly distributed over a network area of 1000m x 1000m, respectively. The BS is located at the centre of the network. 10% of the system nodes is sinkhole nodes. There is not any malicious node in the first round. After the first round, sinkhole nodes come to existence every 10 rounds. The energy model used in this paper is the same as LEACH protocol. The threshold values used by BS in order to determine to send QUERY message is chosen as 0.0001 (as a low value), 0.17 (as a high value) and average amount of energy consumed in the previous round.

Table 3. Simulation Parameters

Parameter	Value
Network Area	1000m x 1000m
Number of Nodes	50, 100, 150 and 200
Coordinates of BS	(500,500)
Initial Energy of Nodes	4J
Distribution of Nodes	Random
Control/Broadcast Message Size (X)	500 bit
Data Message Size (4X)	2000 bit
Sinkhole Ratio	10%
Sinkhole Frequency	every 10 rounds
Energy Threshold	0.0001, 0.17 and average amount of energy consumed in the previous round

Results and Discussion

After modelling the sinkhole attack on different levels of LEACH, cost of the damage is evaluated by measuring total energy consumed in the system, the number of packets reaches up to BS and the number of living nodes for different values of the number of system nodes, including 50, 100, 150 and 200, as is seen in Figure 4 through Figure 6, respectively. The performance of the system under sinkhole attack is compared with the system in safe mode, where an attack does not exist.

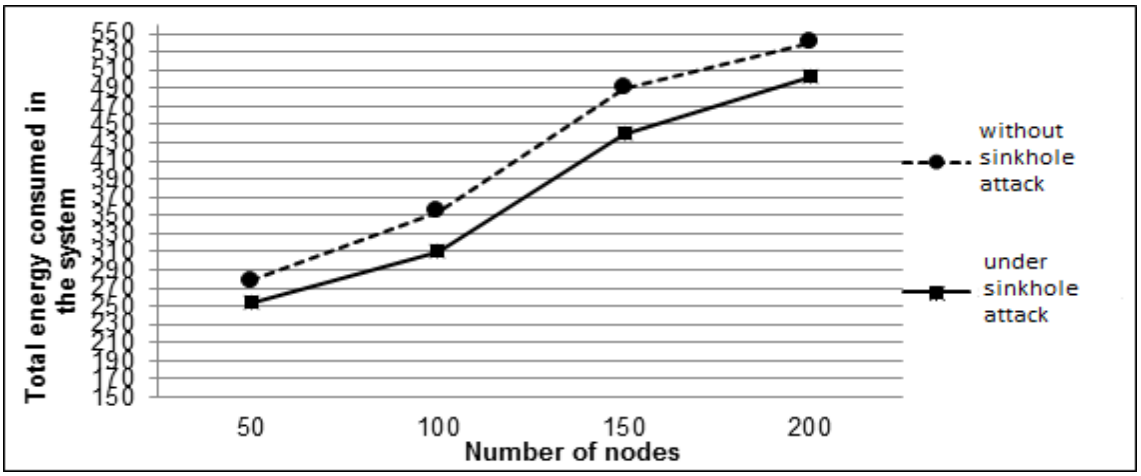

Figure 4. Total energy consumption of the nodes when the system is under sinkhole attack and is in safe mode for a 50,100,150 and 200 numbers of nodes.

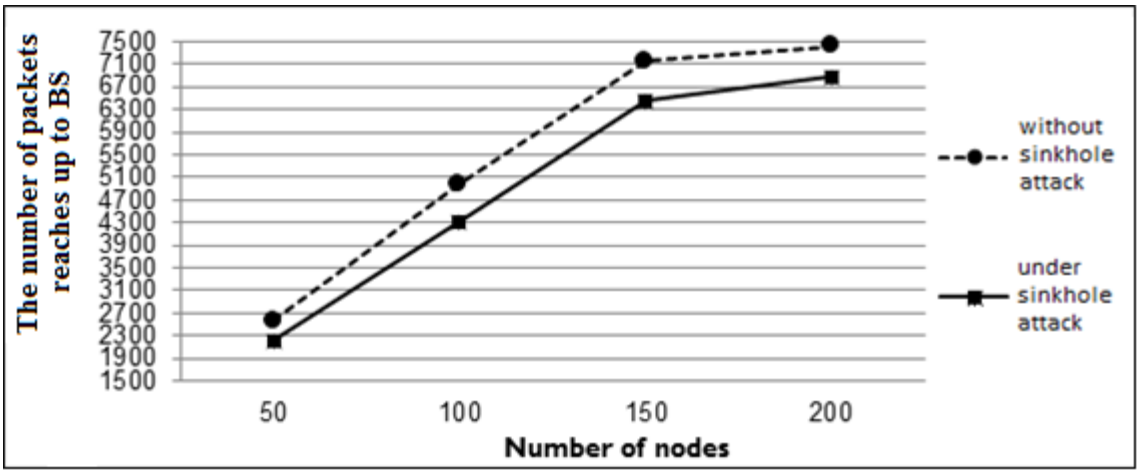

Figure 5. The number of packets arrived at BS when the system is under sinkhole attack and is in safe mode for a 50,100,150 and 200 numbers of nodes.

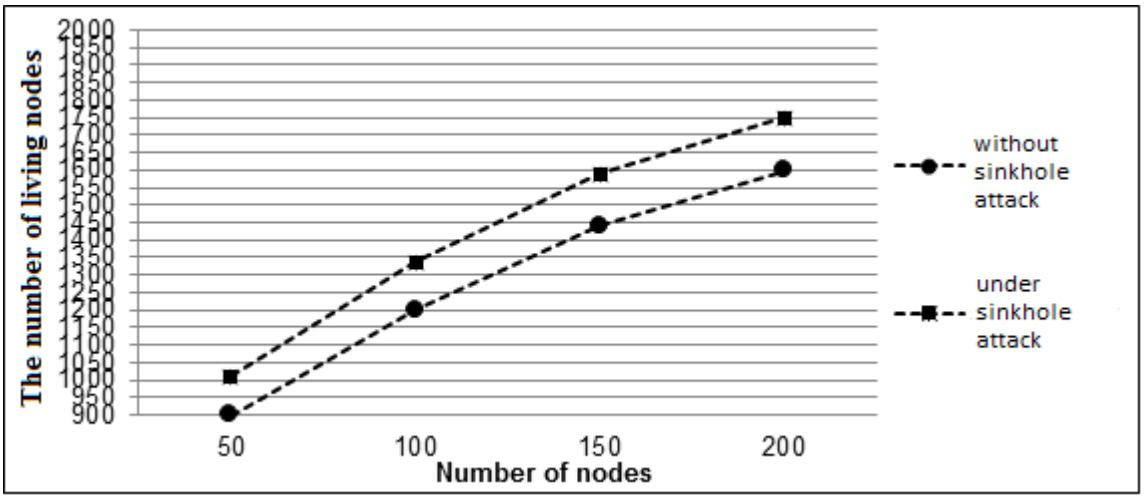

Figure 6. The number of living nodes when the system is under sinkhole attack and is in safe mode for a 50,100,150 and 200 numbers of nodes.

Regardless of the number of nodes in the system, total amount of energy consumed in the system under sinkhole attack is less than the system without any attack, as is seen in Figure 4. According to these results, the malicious node seems to contribute to the lifetime of the network by providing less energy consumption to the nodes. However, in reality, the sinkhole node does not increase the performance of the network but blocks packet transmissions to BS and accordingly, less packets then expected reaches up to BS, as is seen in Figure 5. Besides, loss rate in the packets increases as the number of nodes increases in the system, because the more numbers of the nodes in the system means the more numbers of the infected nodes. By blocking the packet transmission, the malicious node also triggers the system nodes to switch into idle state and correspondingly, do not consume energy to send data and live longer as is seen in Figure 6.

For detecting the sinkhole attack, initially, BS compares the remaining energy level of the suspicious nodes in the list with a certain threshold value and then take further actions if needed. Figure 7 shows total energy consumed in a 50 node system for detecting the attack for different values of thresholds, including 0.0001, average amount of energy consumed in the previous round and 0.17. The results compared with a system without any detection mechanism.

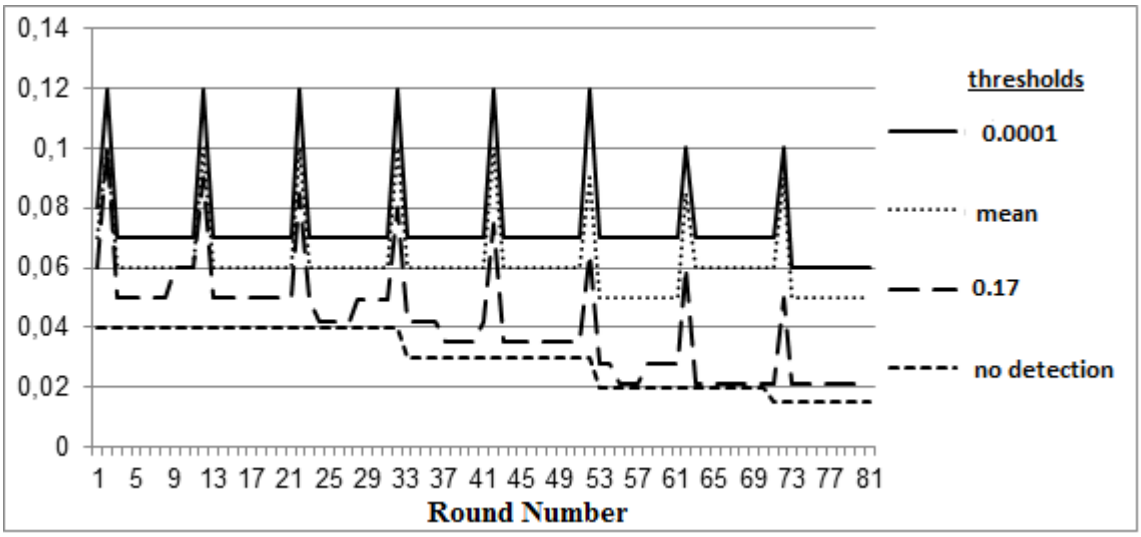

Figure 7. Total energy consumption on a 50 node system for detecting the sinkhole attack for different values of thresholds, including 0.0001, average amount of energy consumed in the previous round and 0.17. The results compared with a system without any detection mechanism.

As is seen in Figure 7, regardless of the threshold value, if any detection mechanism is included in the system, an extra energy is consumed to determine if there is a malicious behaviour in the system or not, as expected. However, the issue is not solely spending less energy, but detecting the sinkhole node with high accuracy and with minimum energy consumption.

Malicious nodes are included 1 in every 10 round, which provokes overshooting in Figure 7. The detection mechanism consumes the energy for only query-response messages. Hence, the more control packets results in the more energy consumption. Maximum energy, which is 59% more than the system without any detection mechanism, is consumed when the threshold is minimum, i.e. 0.0001. The reason is that BS sends more query messages to the suspicious nodes for smaller threshold values and accordingly, consumes much more energy. Similarly, minimum energy, which is 27% more than the system without any detection mechanism, is consumed when the threshold is maximum, i.e. 0.17. In case of using average amount of energy consumed by the system nodes in the previous round as a threshold value, the consumed energy is 46% more than the system without any detection mechanism. If the only evaluation criteria had been the consumed energy, using higher threshold values would have supplied higher system performance. However, investigating the system through different parameters, including the number of packets reaches up to BS and rate of detection of the sinkhole node(s) is significant for the proposed algorithm.

Table 4 shows the number of packets arrived at BS and rate of detection of the sinkhole node(s) for a 50-node system. As is seen in Table 4, although higher threshold values (i.e. 0.17) provide less energy consumption, all of the malicious nodes could not be detected and also packet losses come into existence for these values. This is because BS considers the malicious node as a normal system node and does not send query messages for higher threshold values. If any detection algorithm is not included in the system, since the malicious nodes cannot be detected, packet loss rates figure out at its highest values, as expected. When the threshold value is chosen as minimum or average amount of energy consumed in the previous round, the detection rate is 100%, which means that whole malicious nodes are detected, and also the number of packets

reaches up to BS gets its highest values. Since using lower threshold values results in consuming more energy, optimum threshold value for a 50 node system is determined as average amount of energy consumed in the previous round.

Table 4. The number of packets arrived at BS and rate of detection of the sinkhole node(s) for different values of threshold values on a 50-node system.

Threshold	**# of packets arrived at BS**	**Percentage of Detected Nodes**
0.0001	1901	%100
Mean	1901	%100
0.17	1610	%95
No Detection	674	%0

Figure 8 through Figure 10 shows total energy consumption on a 100, 150 and 200 node system for detecting the attack for different values of thresholds, including 0.0001, average amount of energy consumed in the previous round and 0.17, respectively. Similarly, Table 5 through Table 7 shows the number of packets arrived at BS and rate of detection of the sinkhole node(s) for different values of threshold values on a 100, 150 and 200 node system, respectively. The results compared with a system without any detection mechanism.

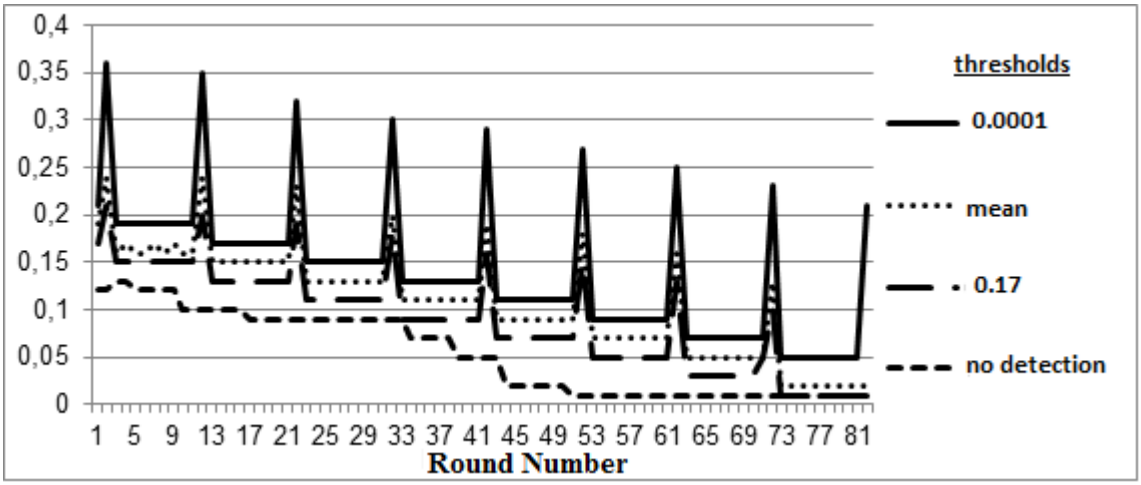

Figure 8. Total energy consumption on a 100 node system for detecting the sinkhole attack for different values of thresholds. The results compared with a system without any detection mechanism.

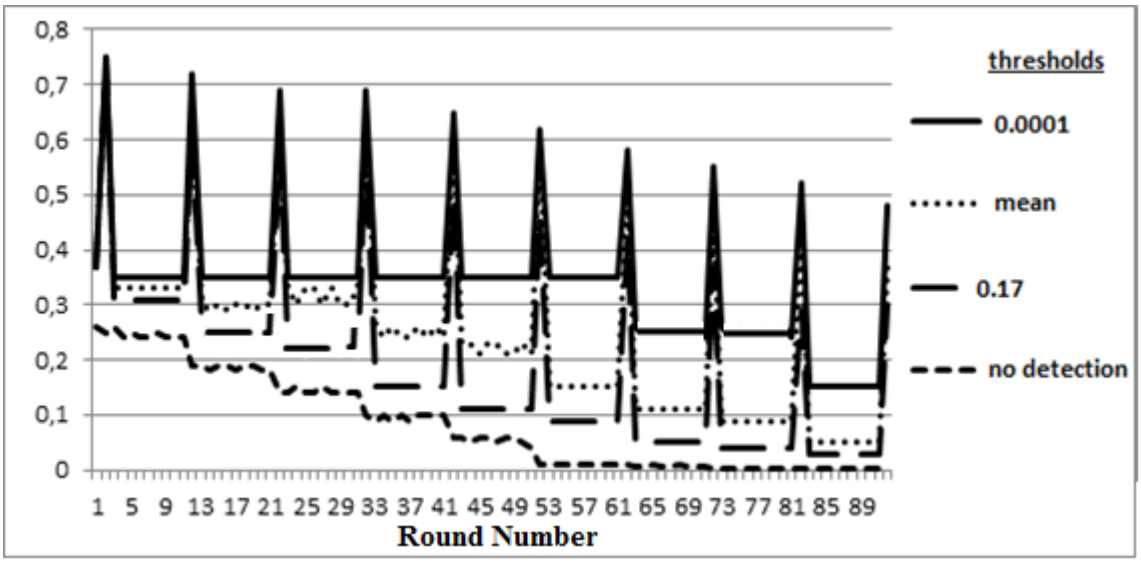

Figure 9. Total energy consumption on a 150 node system for detecting the sinkhole attack for different values of thresholds. The results compared with a system without any detection mechanism.

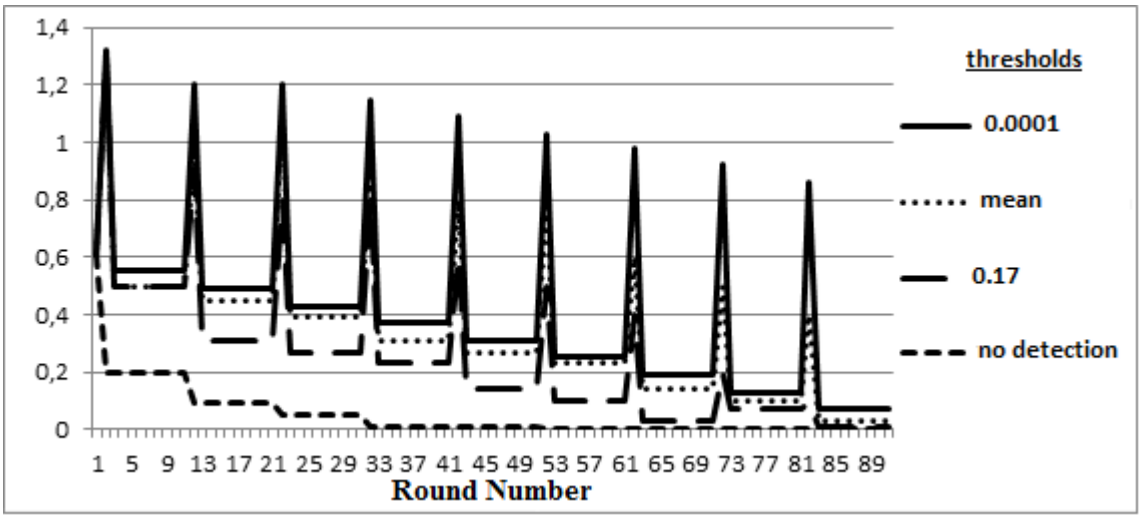

Figure 10. Total energy consumption on a 200 node system for detecting the sinkhole attack for different values of thresholds. The results compared with a system without any detection mechanism.

As is seen in Figures, as the number of nodes increases, total energy consumed by the system for detecting the malicious nodes increases regardless of the threshold values since the more number of system nodes causes the more number of malicious nodes and accordingly the more number of query-response messages.

Table 5. The number of packets arrived at BS and rate of detection of the sinkhole node(s) for different values of threshold values on a 100-node system.

Threshold	# of packets arrived at BS	Percentage of Detected Nodes
0.0001	5056	%100
Mean	5056	%100
0.17	3800	%65
No Detection	1981	%0

Table 6. The number of packets arrived at BS and rate of detection of the sinkhole node(s) for different values of threshold values on a 150-node system.

Threshold	# of packets arrived at BS	Percentage of Detected Nodes
0.0001	6373	%100
Mean	6373	%100
0.17	5436	%60
No Detection	2438	%0

Table 7. The number of packets arrived at BS and rate of detection of the sinkhole node(s) for different values of threshold values on a 200-node system.

Threshold	# of packets arrived at BS	Percentage of Detected Nodes
0.0001	9003	%100
Mean	8967	%100
0.17	6500	%55
No Detection	3907	%0

As is seen in Tables, regardless of the threshold values, the number of packets arrived at BS increases as the number of nodes in the system increases since the more number of nodes states the more number of packets created by the system. While detection rate of the highest threshold value decreases as the number of nodes increases, that of lower threshold values remains as the highest accuracy rate, i.e. 100%. The results show that higher threshold values are not suitable for higher number of nodes. The threshold of average amount of energy consumed in the previous round is the best choice regardless of the numbers of nodes in the system due to providing higher accuracy (100%) and more numbers of packets to be gathered by BS than higher thresholds with lower energy consumption than lower thresholds.

Conclusion

Due to locating in harsh and/or hostile environment and having limited resources, WSNs are open to attacks. Since one of the most dangerous attacks threatening WSN is the sinkhole attack,

various studies have been proposed in literature on detecting this type of attack. In this study, a centralized detection algorithm based on the remaining energies of the nodes on cluster-based WSNs is proposed. BS tracks the packet transmissions and list the nodes that did not send packets on current round. By comparing the remaining energy of the suspicious nodes in the list with a certain threshold value, BS determines to take a further action or not. ıf the node is marked as malicious, then an alarm message is created to warn the system nodes. After conducting a number of simulations for different numbers of nodes, it is observed that optimum threshold value that reaches high accuracy rates with consuming minimum energy is average amount of energy consumed in the previous round.

References

Bahekmat, M., Yaghmaee, M. H., Yazdi, A. S. H., & Sadeghi, S. (2012). A Novel Algorithm for Detecting Sinkhole Attacks in WSNs. *International Journal of Computer Theory and Engineering*, *4*(3), 418-421.

Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), 266-282.

Chaudhry, J. A., Tariq, U., Amin, M. A., & Rittenhouse, R. G. (2013). Dealing with Sinkhole Attacks in Wireless Sensor Networks. *Advanced Science and Technology Letters*, *29*, 7-12.

Chen, C., Song, M., & Hsieh, G. (2010, June). Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. In *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on* (pp. 711-716). IEEE.

Gondwal, N., & Diwaker, C. (2013). Detecting blackhole attack in WSN by check agent using multiple base stations. American International Journal of Research in Science, Technology, Engineering & Mathematics, 3(2), 149-152.

Han, G., Li, X., Jiang, J., Shu, L., & Lloret, J. (2014). Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks. *The Computer Journal*, bxu036.

Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. InSystem sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on (pp. 10-pp). IEEE.

Ngai, E. C., Liu, J., & Lyu, M. R. (2007). An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications*, *30*(11), 2353-2364.

Papadimitriou, A., Le Fessant, F., Viana, A. C., & Sengul, C. (2009, October). Cryptographic protocols to fight sinkhole attacks on tree-based routing in wireless sensor networks. In *Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on* (pp. 43-48). IEEE.

Patil, S. S., & Khanagoudar, P. S. (2012). Intrusion Detection Based Security Solution for Cluster Based WSN. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, *1*(4), pp-331.

Radhikabaskar, D. P., Komara, S., & Paul, V. (2014) Sinkhole Attack Detection In Hierarchical Sensor Networks. International Journal of Scientific & Engineering Research, Volume 5, Issue 9.

Sharmila, S., & Umamaheswari, G. (2011, July). Detection of sinkhole attack in wireless sensor networks using message digest algorithms. In *Process Automation, Control and Computing (PACC), 2011 International Conference on*(pp. 1-6). IEEE.

Singh, S. K., Singh, M. P., & Singh, D. K. (2011). Intrusion detection based security solution for cluster-based wireless sensor networks. *International Journal of Advanced Science and Technology*, *30*(83).

Varga, Andras. "OMNeT++." Modeling and Tools for Network Simulation (2010): 35-59.

Xing, K., Srinivasan, S. S. R., Jose, M., Li, J., & Cheng, X. (2010). Attacks and countermeasures in sensor networks: a survey. In Network security (pp. 251-272). Springer US.