Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 15 Issue 7 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security Issues and Energy Consumption in Implementing Wireless Sensor Networks

By Sameer Alalawi & Zenon Chaczko
University of Technology, Australia

Abstract- The Internet has become an indispensable means of sourcing and storing information. In the future, the Internet will be used to control objects, not just information. This raises the issue of security. In the case of wireless sensor networks, the main challenge will be to provide secure lines of communication between devices on the same network.

Keywords: WSNs; attacks; threats; sinkhole attack; hello flood attack.

GJCST-E Classification : C.2.1 D.4.6 C.2.5

SECURITYISSUESANDENERGYCONSUMPTIONINIMPLEMENTINGWIRELESSSENSORNETWORKS

Strictly as per the compliance and regulations of:

Security Issues and Energy Consumption in Implementing Wireless Sensor Networks

Sameer Alalawi [α] & Zenon Chaczko [σ]

Abstract- The Internet has become an indispensable means of sourcing and storing information. In the future, the Internet will be used to control objects, not just information. This raises the issue of security. In the case of wireless sensor networks, the main challenge will be to provide secure lines of communication between devices on the same network.

Keywords: WSNs; attacks; threats; sinkhole attack; hello flood attack.

I. Introduction

Sensors have been implemented to read information from physical devices in order to use this information for multiple purposes. Sensors convert analog signals to digital signals for processing and computation purposes. 'A sensor is a type of transducer that converts energy in the physical world into electrical energy that can be passed to a computing system or controller' (Dargie et al. 2010 p. 4). Furthermore, sensors have the ability to send and receive information to other sensors in the same area, creating a network between several sensors. This is called a wireless sensor network (WSN), which is 'a group of sensors cooperatively monitoring a large physical environment' (Dargie et al. 2010 p. 7). While a Wireless sensor network provides full controlling on devices by sending and receiving information between them, it requires strong security mechanisms against the threats of attackers. In this way, implementing wired security mechanisms in a WSN is an inefficient solution. Bashir & Hussain (2013) indicate that providing security protocols for WSNs is a big challenge due to the resource constraints of the WSN itself. Furthermore, Boukerch et al. (2007) point out that the reason of inefficiency of using the wired or wireless security mechanisms in a WSN is the CPU computations, delay constraints and the communications of applications that run on the top of that network. Applying traditional security mechanisms in WSNs increases the delay of transferring information and causes packets of information to go missing when transferring in WSN communication.

Network security requires four mechanisms in order to control the resources and keep these resources safe. These mechanisms are confidentiality, integrity, authentication and availability. Each mechanism requires certain protocols, which are working together to achieve these four security goals. The perfect solution to prevent attacks is to understand the behaviour of their threats and protect the resources against these attacks. Several papers explain threats to WSNs and classify them into more than one class. Tahir & Shah (2008) classify threats in WSNs into two classes. The first are mote class attackers, the second are laptop-class attackers. The attackers are further categorised into four dimensions: motive, determination, knowledge and resources. Threats in WSNs can also be categorized depending on the OSI model layers. This classification is useful in troubleshooting and maintenance purposes. In addition, the OSI model simplifies the detection of the attacking, which is the most difficult step to detect the threats. Sarma & Kar (2006) indicate some examples of threats, which relate to the OSI layers, such as the physical layer which is threatened by jamming and tampering, the data link layer which is threatened by the collision or exhaustion, and the network layer which is threatened by routing protocol. This report discusses some proposed solutions of the security mechanisms and provides the results of a simulation for sinkhole and hello flood attacks which WSNs are susceptible to. The first section provides background and reviews the threats in the WSN, the second section explains the method used to examine the behaviour of sensors under threat, the third section views the results of this simulation, the fourth section discusses the results of the simulation for examining the sinkhole and hello flood attacks and provides solutions to these threats.

II. Literature Review/Background

Several papers discuss the threats to WSNs as a big issue in creating a network design. Path et al. (2006) mention that most threats to WSNs are similar to those that threaten wireless networks, but some are specific to WSNs. However, the security solutions for wireless networks cannot be applied successfully to wireless sensor networks due to the architectural dissimilarities of these two networks. Tahir & Shah (2008) point out some common security threats, which attack sensor nodes in WSNs. The first threat is a sleep duration attack; this attack happens during the changing from active to sleep mode. The main purpose of this attack is to prevent sensor nodes from energy saving while it is in a sleep mode in order to reduce the power

Author α σ : Technical and Vocational Training Corporation (TVTC) KSA, University of Technology, Sydney (UTS).
e-mails: s.alshoikan@tvtc.gov.sa, Czenon.Chaczho@uts.edu.au

resources (Tahir & Shah 2008). Consequently, the attacker controls other sensors by International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct. -2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 15 sending a request, which makes it appear as if the sensor is dead. Another threat is the sinkhole attack. The attacker in a sinkhole attack attracts all routing paths towards itself. Pathan, Lee & Hong (2006) indicate that some malicious nodes try to attract all the traffic in the sensor network. In a flooding based control, the attackers receive a request for routing and send it to the target node. Malicious nodes will be able to control the packets transferring between nodes, while it involves itself between them. The third threat to WSNs is the wormhole attack .The attacker in this threat records the packets at one of the locations and transfers these packets to another location. Tahir & Shah (2008) point out that this kind of threat gives the malicious nodes in the WSN the observation to attract the other nodes for routing. The sybil attack is another kind of threat to WSNs. This attack tries to tamper with the integrity of data in order to attack the distribution storage, routing protocol and data aggregation. This attack occurs by using fake locations of multiple identities. Consequently, the attacker will be located in multiple locations with different identities. The fifth threat is the hello flood attack; this attack uses hello packets as a sign to attack the sensor nodes. Hello flood attack is a laptop class (Tahir & Shah 2008). While the hello message is a crucial sign for establishing a successful communication between neighbours' nodes, the attacker who uses hello flood attack tries to announce itself to be one of the neighbours of other nodes in order to involve itself in the attacking network. Denial of service attack is also considered as one of the threats in network design. The main idea of this threat is that the attacker tries to exhaust all resources in the attacking network by sending a large number of unnecessary packets. Tahir & Shah (2008) discuss a kind of denial of service attacks called a jamming attack. A jamming attack tries to jam the communication between sensor nodes. Thus, these previous threats attack the software of nodes communication in the WSN considering on the routing protocols.

Some threats attack the hardware of sensors instead of software. Adnan, Yussoff & Hashim (2010) point out the physical prospective threats to WSNs, which is attacking the initial boot phase of the devices. Another threat is passive information gathering, which collects information from nodes, while the data is not encrypted. Tahir & Shah (2008) indicate that attackers can destroy sensors by extracting the physical location especially if the attacker is a laptop class. The authors recommend a combination between hardware security solutions with software security solutions in wireless sensor networks, to enhance the security level in the system.

III. Sinkhole Attack

A sinkhole attack targets the sink nodes in order to persuade all traffic through it for stealing the nodes' information. Hamedheidari & Rafeh (2013) indicate that the goal of a sinkhole attack is to change the routing paths from one area to another. In a WSN, creating sinkhole attacks is easy because the routing topology in this network is based on tree routing. Tree based routing topology increases the impact of malicious nodes, which are dependent on the number of uncompromised sensors. Hamedheidari & Rafeh (2013) explain the way of launching sinkhole attacks in distance vector routing protocol (AODV); this routing method depends on hop count to find the shortest path to the base station. The malicious node in this case sends a message to the sender telling it its path is the best and shortest path to the base station. Consequently, the attacker node collects all data coming through it. Furthermore, sinkhole attacks prevent the base station from getting correct data from neighbours (Sreelaja & Pai 2014). This is the result of persuading all routing paths neighbours to the attacking nodes. However, the detection of sinkhole attacking node is difficult because the attacker uses the right authentication of the normal sensor to establish a communication with neighbours. The attacker in a sinkhole threat can affect the sink node and establish the attack in two ways. The first type is malicious insider, while the second type is resourceful outsider. Shafiei et al. (2014) point out that the attacker uses a malicious node to start the attacking by deceiving neighbours that the compromised node is the best path to the base station. As the result of that, laptop class malicious node, which is equipped with high performance, leads the network route from the right paths to the malicious node path. The high performance malicious node may attract most surrounding nodes to the sinkhole (Shafiei et al. 2014). Furthermore, sinkhole may threaten by using a wormhole attack after capturing all packets from the sink nodes' neighbours and using a tunnel to transfer packets to the other nodes, which is colluded to the malicious node. The main job of the colluded node is sending messages to the base station. Shafiei et al. (2014) indicate that this attack prevents the sender from discovering any routing path except the tunnel, which leads to disruption of the network's functionality.

Several papers proposed means of how to detect and prevent a sinkhole attack. Sreelaja & Pai (2014) explain the swarm inelegance approach of sinkhole threats against hope count routing protocol. This approach detects the sinkhole attack in distance vector routing protocol using a slowly hop count monitoring and an alert method in order to generate the threat on detecting the sinkhole attack. On the other hand, Hamedheidari & Rafeh (2014) proposed a trust model to detect the attacking nodes and prevent the threats; this trust node uses three codes before establishing the communication between sensors. However, these approaches are inefficient in WSNs due to the mobility of nodes; which is the most important method for WSNs in distance vector International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 16 protocol. This is because the mobility of nodes may leave some nodes without covering of any agents; uncovered nodes are considered unreliable, which makes it possible for malicious nodes to attack this unreliable node (Hamedheidari & Rafeh 2014). However, Fessant et al. (2012) analyse two protocols that increase the network performance with the existence of the sinkhole attack. These protocols are ERSIST-1 and ERSIST-0. While ERSIST-0 prevents malicious nodes from lying about their advertised distance, ERSIST-1 stops the lying about their advertised distance.

IV. Simple Configuration Protocol (Resist 1)

This protocol uses the hello messages, which consist of epoch-tokens as a trust key to all neighbours. The sensor chooses one of the following when it receives the hello message:

1. If the epoch is new, that means it receives the current epoch and it has to send the next one to the shortest path.
2. If the epoch is already taken, the node updates itself and propagates a new hello message to the neighbours.

This protocol guarantees that the sinkhole attack forwards the messages without dropping the first epoch-token.

V. Complex Configuration Protocol (Resist 0)

This protocol uses the same of ERSIST-1 but the sensor challenges its parents before sending the hello messages by using public and private keys. This approach is useful while the malicious node does not have the private key of the sinkhole. Furthermore, dropping the packets does not succeed because neighbour nodes would not respond to the challenge if it does not match.

Fessant et al. (2012) indicate that signing the key is an issue in WSNs due to the lack of memory. However, there are several approaches that are proposed to design key management such as LEDs but they still need to be more efficient to work in WSNs.

VI. Hello Flood Attack in Wireless Sensor Networks

WSNs depend on certain protocols to manage the communication between nodes. Nodes in this network use hello packets in order to communicate with their neighbours and calculate the best path routing to the base station. However, the attackers use this protocol to threaten the network topology by introducing a malicious node to the other nodes in the range and spread its threat to the rest of the nodes in the attacked network. Hello flooding attack is designed to exploit the broadcasting nature of these protocols in order to convince a large group of nodes that the sender is a normal neighbour, by using a very high transmit power (Haghighi et al. 2011). A laptop class attacker could persuade all nodes in the network that the attacked node is a normal neighbour. In this way, the attacked node does not need to seem legal for the other nodes in order to attack the network because it can convince the other nodes to follow it by producing a high power signal for broadcasting. After attacking the target node, the attacker uses flooding to spread viruses via broadcast messages to all nodes in the network; " the hello flood attack uses a single hope broadcast to transmit the message to a large number of receivers" (Karlof et al. 2003 p. 302). Furthermore, laptop class uses the hello flood attack to disable the functionality of the target network by changing the power of transmit to reach the lowest value of broadcasting to the other neighbours after convincing these nodes. In this way, several efforts deliver some solutions for the hello flood attacking in a WSN. Karlof & Wagner (2003) point out that verifying the two ways links of every node is one of the solutions for defencing the hello flood attack. However, this solution is inefficient if the malicious node reduces a high power transmit for the other neighbour nodes, due to the high convince of the malicious node. Moreover, authentication is another solution for this issue by challenging all links around the nodes before accepting the hello message. While authentication prevents the hello flood from spreading due to the challenging methods, it does not prevent the compromised nodes from authenticating themselves to their neighbours in the network.

VII. Using Leach Protocol to Detect the Hello Flood Attack

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a technology used for managing the hierarchy of the topology in a WSN. The main goal of LEACH protocol is allowing every node connected to the WSN to reach the base station (Magotra & Kumar 2014). LEACH groups nodes into several clusters; one of the nodes inside the cluster acts as a cluster head. Magotra & Kumar (2014) indicate that LEACH protocol uses random alternation of the nodes to be the cluster head; since the new cluster head takes its position, it sends new hello packets to all neighbours in its range.

Several studies use LEACH protocol to address the hello flood attack and prevent the threats presented by malicious nodes. Magotra & Kumar (2014) classify these studies into two groups; while the first group focuses on cryptographic-based approach, such as FLEACH, S-LEACH and sec-LEACH, the second group focuses on non-cryptographic based International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 17 approaches such as the single strength based detection approach.

The non-cluster head mode is a node without a cluster head agent in LEACH protocol, compares the RSS with the distance between non-CH and any elected CH node. Magotra & Kumar (2014) indicate that nodes whose RSS and distance in the same range are able to join the cluster head. The node calculates the distance to the cluster head depending on this formula:

$$\text{Dis} = \text{sqrt}\,[\text{sq}\,(x2 - x1) + \text{sq}\,(y2 - y1)]$$

Such as, x1 and y1 are the location of nodes receiving packets, x2 and y2 are the location of the cluster head, which is sent via hello packet; this calculation is for the sending and the receiving nodes.

VIII. Hello Flood Attack Detection

LEACH protocol focuses on changing the cluster head regularly to prevent the threats and improve the network performance. Magotra & Kumar (2014) proposed that this changing is based on two parameters. The first parameter focuses on the position of the nodes, while the second parameter focuses on the number random round of choosing a new cluster head in LEACH protocol.

- Attacking node position

It focuses on the nodes position and replaces the malicious node by using LEACH protocol. Three scenarios are used to replace the attacked node with a normal node.

➢ Detection time period: It is the average of time by the total number of nodes in the network in order to detect the malicious node.

➢ Energy required: It is the average of energy by the total number of nodes in the network in order to detect the malicious node.

➢ Communication: It is the number of test packets detecting, which is sent by the malicious node for creating the hello flooding attack.

Magotra & Kumar (2014) indicate that the communication is secure from the hello flooding attack while the test packets transferring between nodes is in the lowest average.

- Number of random rounds in LEACH

The changing of cluster head randomly and regularly between nodes, leads to understand the effect ofmalicious nodes. The result of that is increasing the performance of the WSN even when the nodes are affected by a hello flood attack. This is because the hello flood attack can be detected with low energy and in less time. A low rate of energy leads to increasing the network performance lifetime and detect the hello flood attack (Magotra & Kumar 2014).

IX. Research Methods

The method used for this research is a simulation, which simulates the behaviour of sensors in a WSN under attack. Wise-net simulation is implemented to simulate the communication between nodes in any environment. It helps WSNs designers to examine the routing paths between nodes in the network. We use this simulator to simulate the sensor behaviour under two kinds of attacks. These attacks are sinkhole attack and hello flood attack. The simulation provides several outputs for each test. This project focuses on the energy of the sensor before and after the attack.

X. Results

a) *Normal node*

The normal connection in figure 1 shows the way of routing protocol messages between nodes as well as the energy consumption, which is produced from the base station. Normally, the base station (sink node) provides energy to all sensors, which are located in the same area. Consequently, the sensors communicate with each other using the received energy from the base station. However, the messages transmission in normal nodes simulation records 91%, this percentage is reasonable enough to ensure perfect communication between nodes in the same cluster.

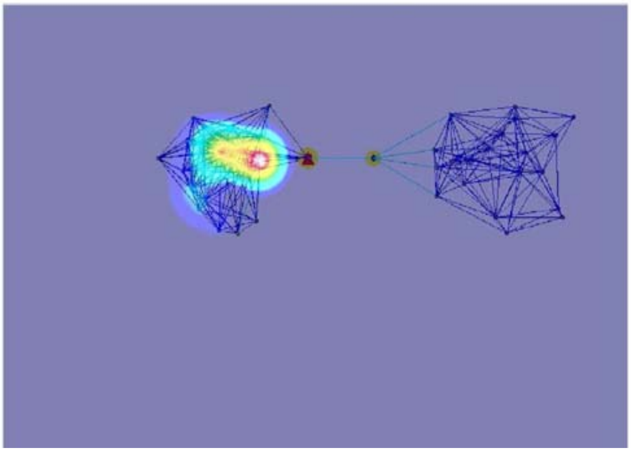


Figure 1: shows the normal energy of the node's connection Security Issues and Energy consumption in Implementing Wireless Sensor Networks November 3, 2014

b) Sinkhole attack nodes

Nodes under a sinkhole attack are unstable and dysfunctional due to the lack of providing the energy needed. Figure 3 shows the energy chart of nodes under a sinkhole attack. It shows losing of energy especially in the core of the network topology. This is because the malicious node tries to persuade all routing paths toward itself, which results in a confusion in sending and receiving information between nodes. For example, a normal node changes the routing request from the correct path to the wrong path by using a malicious node. This is because the International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 18 malicious node attracts nodes in that area that its path is the best path to the base station by using a highenergy output. Figure 3 shows that the transmission and routing feedback are dropped compared with the normal node's situation.

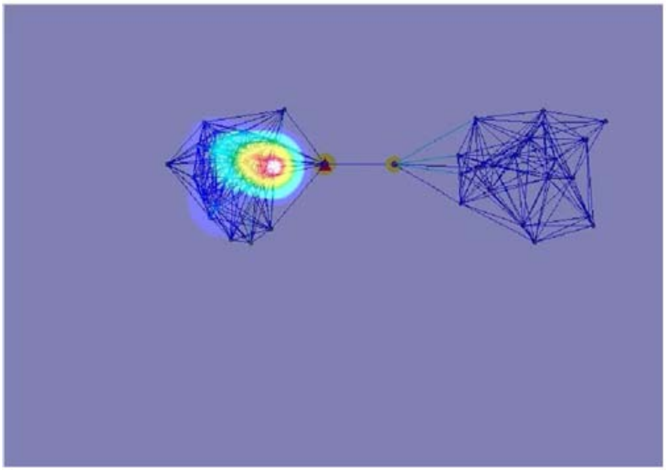


Figure 2 : shows the nodes energy under sinkhole attack

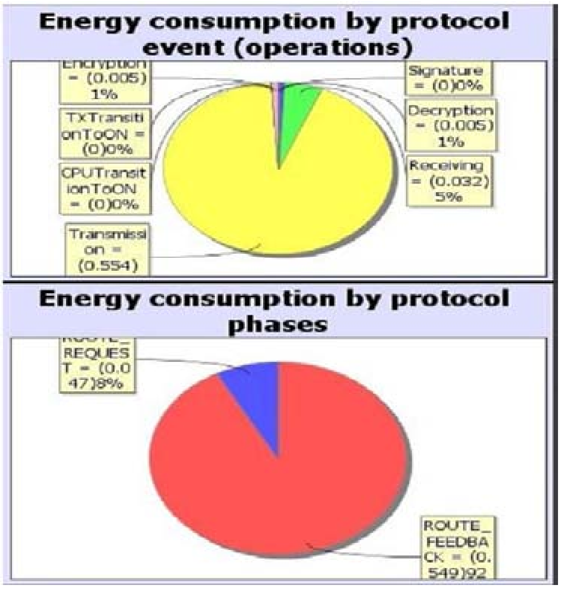


Figure 3 : shows a chart of energy consumption under sinkhole attack

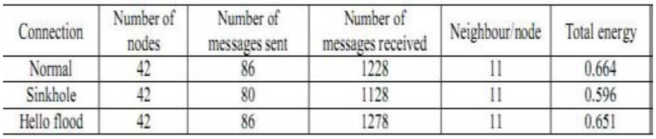
Security Issues and Energy consumption in Implementing Wireless Sensor Networks November 3, 2014

c) Hello flood attack node

The malicious node in hello flood attack provides different mechanisms to the nodes in the network for attacking the network. Figure (4) shows that the energy distribution of sensors has changed due to the attacking. The malicious node in hello flood attack divides the energy consumption into two parts in this network. This is because the hello flood attack tries to separate the network then control each part separately in order to lose the energy of sensors. Figure 5 shows that the transmission between nodes under hello flood attack is decreasing compared with the normal nodes, but the route feedback is increased compared with nodes under sinkhole attack. This is because hello flood focuses on sending and receiving messages between nodes to persuade them that the malicious node is the best path to the base station.

XI. Routing Information

In this section the base station is chosen to examine the output of its routing information for all three types of connection; normal connection, sinkhole attack connection and hello flood attack connection. We examine all connection cases with 12 simulation nodes and 11 neighbours as shown in table (1). From the results we found that the energy in normal connection is the highest than all of the other connections; this is normal because the energy is distributed to all nodes equally. On the other hand, the number of messages received in hello flood attack connection is the highest number comparing with the other connections, due to the behaviour of the malicious node in this attack.



Connection	Number of nodes	Number of messages sent	Number of messages received	Neighbour/node	Total energy
Normal	42	86	1228	11	0.664
Sinkhole	42	80	1128	11	0.596
Hello flood	42	86	1278	11	0.651

XII. Discussion

From the results of these simulations we found that that the energy is changed consequently with the changing of node behaviour. These threats affect the network energy which leads to changing the correct routing path for sending and receiving the information in order to connect to the base station. While wireless security mechanisms defend against the threats and provide a good protection for the network design, these mechanisms in wireless sensor networks need to add some new features for sending and receiving information in a secure way. This is because the security mechanisms require memory and CPU for computation and finding results. In this area using routing protocol, which protects the communication between sensors nodes by adding a secure header for all packets transferring is one of the proposed solutions. On the other side, LEACH protocol is also a good method to secure a wireless sensor network, by changing the base station regularly to ensure that the attacked node is changing if it is affected by any threat. Furthermore, using 6LOW-PAN protocol with low power consumption in routing protocol is a part of this solution to prevent the lack of energy. However, these changes of nodes and routing methods need to be adjustable with the threats affecting the rank of sensors, this is because these changes lead to the weakening of the cryptographic solution.

XIII. Conclusion

WSNs are the basic technology for building networks of devices that can be controlled via the Internet. The sensor technology converts analog signals such as sound or light to digital signals for computation and International Journal of Industrial Electronics and Electrical Engineering, ISSN: 2347-6982 Volume-3, Issue-10, Oct.-2015 Security Issues And Energy Consumption In Implementing Wireless Sensor Networks 19 communication. The communication between sensors requires an efficient design to create a WSN topology. For example, using clusters to divide the sensor nodes into several parts in order to organize the network resources. This report has discussed some of the challenges for creating an efficient and reliable wireless sensor network by reviewing and discussing the security issues in implementing the topology of WSN design. From the examination of two kinds of attacks in WSNs, we found that the energy distribution of sensors is disrupted in consequence of the threat, which is caused by the malicious nodes. For example, the sinkhole attack tries to persuade all routing traffic toward itself in order to capture all information of nodes. This is because the attacker changes the energy power producer from the base station (sink-node) to the malicious node. Another example for examining the threat in a WSN is the hello flood attack. This attack uses the hello flood attack to send affected messages to its neighbours. From the simulation of hello flood attack, we found that the power consumption of the sensor in one cluster is divided into two parts, which allows the malicious node to control each part separately by dividing the power after attacking.

Several papers propose some mechanisms for implementing a secure WSN. LEACH protocol is one of these mechanisms, which considers in changing the base station regularly. While this mechanism solves some attacks and helps the network designers to create a secure WSN, it causes instability in the network in consequence of changing the routing methods. On the other hand, using an epoch-token as a trust key is another mechanism proposed to solve the security issue in wireless sensor network. This mechanism is successful in detecting the sinkhole attack, because it sends and receives the pre-shared key between the node and its base station. However, no paper until now has proposed how to detect the other threats, such as hello flood or denial of services using the epoch-token mechanism. All attacks focuses on the energy for persuading the other nodes that the malicious node is the best path to the base station. For that reason, implementing a trust model for energy with these mechanisms of security may solve that problem. For example, Use 6- LOWPAN routing protocol, which consumes low power in routing method between sensors, may leads to stop the sensors searching for the highest power in the cluster for sending the information.

Reference Reference Referencias

1. Adnan, L.H., Yussoff, Y.M. & Hashim, H. 2010,'Secure Boot Process for Wireless Sensor Node', International Conference on Computer Applications and Industrial Electronics (ICCAIE), pp. 646- 649.
2. Boukerch, A., Xu, L. & El-khatib, K. 2007,'Trusted-based security for wireless as hoc and sensor networks', computer communications, vol. 30, pp. 2413-2427.
3. Bashir, A. & Mir, A.S. 2013,'An Energy Efficient and Dynamic Security Protocol for Wireless Sensor Network', International Conference on Advance Electronic System (ICAES), pp. 257-261.
4. Badakhshan, M. & Arifler, D. 2007,'Simulation Based Analysis of Spreading Dynamic of Malware in Wireless Sensor Network', International Conference on Sensor Technologies and Applications, vol. 65, pp. 164-169.

5. Dargi, W. & Poellabauer, C. 2010, Fundamentals of Wireless Sensor Networks, 1st edn, Wiley Series on Wireless Communications and Mobile Computing, John Wiley & Sons Ltd, Chichester, UK.
6. Fessant, F.L., Papadimitriou, A., Viana, A.C., Sengul, C. & Palomar, E. 2012,'A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis', Computer Communications, vol. 35, pp. 234-248.
7. Haghighi, M.S., Mohamedpour, K., Varadharajan, V. Quinn, B.G. 2011,'Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks', Transaction on Information Forensics and Security, vol. 6, no. 4, pp. 1185-1199.
8. Hamedheidari, S. & Rafeh, R. 2013,'A novel agent-based approach to detect sinkhole attacks in wireless sensor network', Computer & Security, vol. 37, pp. 1-14.
9. Sreelaja, N.K. & Pai, G.A.V. 2014,'Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks', Applied Soft Computing, vol. 19, pp. 68- 79.
10. Karlof, C. & Wagner, D. 2003,'Secure routing in wireless sensor network: attacks and countermeasures', Ad Hoc Networks, vol. 1, pp. 293-315.
11. Magotra, S. & Kumar, K. 2014,'Detection of HELLO flood attack on LEACH protocol', International Advance Computing Conference (IACC), pp. 193-198.
12. Pathan, A.K., Lee, H & Hong, C.S. 2006,'Security in Wireless Sensor Network: Issues and Challengies', ISBN, pp. 1043-1048.
13. Sarma, H.K.D & Kar, A. 2006,'Security Threats in Wireless Sensor Networks', IEEE, pp. 243-251.
14. Sarma, H.K.D & Kar, A. 2008,'Security Threats in Wireless Sensor Networks', IEE A&E System Magazine, Jun, pp. 39- 45.
15. Shafiei, H., Khonsari, A., Derakhshi, H. & Mousavi, P. 2014,'Detection and mitigation of sinkhole attacks in wireless sensor network', Journal of Computer and System Science, vol. 80, pp. 644-653.
16. Stafrace, S.K. & Antonopoulos, N. 2010,'Malitary tactics in agent-based sinkhole attack detection for wireless ad hoc networks', computer Communications, vol. 33, pp. 619-638.
17. Tahir, H. & Shah, S.A.A. 2008,'Wireless Sensor Networks-A Security Prespective', IEEE, pp. 189-193.
18. Wang, Y., Lin, W. & Zhang, T. 2010,'Study on Security of Wireless Sensor Networks in Smart Grid', International Conference on Power Technology, pp. 1-7.
19. Zhang, X., He, J. & Wei, Q. 2009,'Security Considerations on Node Mobility in Wireless Sensor Networks', Fourth International Conference on Computer Science and Convergence Information Technology, vol. 275, pp. 1143-1146.
20. Zhang, F., Zhai, L., Yang, J. & Cui, X. 2014,'Sinkhole attack detection based on redundancy mechanism in wireless sensor network', Information Technology in Quantitative Management (ITQM), vol. 31, pp. 711-720.