Sinkhole Attack in Wireless Sensor Networks- Performance Analysis and Detection Methods

Radhika Baskar, P. C. Kishore Raja, Christeena Joseph and M. Reji

Department of Electronics and Communication Engineering, Saveetha University, Chennai – 600077, Tamil Nadu, India; radhikabaskr@gmail.com, pckishoreraja@gmail.com, Christeena003@gmail.com, rejime@gmail.com

Abstract

Objectives: Wireless sensor networks are used, especially in military, tracking and monitoring applications. Security systems play an important role as the wireless nature is susceptible to attacks. The main idea is to analyse the performance of the network when subjected to sinkhole attack for various scenarios. Methods/Statistical Analysis: Limited energy, computational capacity and storage are some of the constraints on sensor networks which make it to analyze in a different way compared to adhoc networks. In this paper, we discuss the various attacks and attributes which are used to detect the attacks and present a simulation on the effect of sinkhole attack based on various set of parameters. The performance of the system is analyzed when the network is being subjected to sinkhole attack considering the scenarios of varying network size, number of compromised node, intruder power and the location of the sinkhole attack. The available detection methods of the sinkhole attack are tabulated. Findings: Parameters such as average energy consumption, throughput and packet delivery ratio are analyzed. It is seen that the network performance is degraded by the implementation of the attack and there is a decrease in parameters analyzed when subjected to various scenarios. Application/ Improvement: The variation of the parameters in the attack scenarios will be useful in formulating a detection algorithm. The network can be analysed for different scenarios and more number of parameters.

Keywords: Attack, Packet Delivery Ratio, Performance Analysis, Sensor Network, Sinkhole, Throughput

1. Introduction

A Wireless Sensor Network (WSN) comprises large number of low – power, low cost, multifunctional and spatially distributed sensor nodes, which are densely deployed to continuously monitor physical or environmental conditions. Sensor nodes also referred as motes, obtain surrounding data by the measurement of physical parameters such as pressure, temperature, relative humidity etc., and forward the sensing data to base station which acts as a sink. WSN is either structured or unstructured. Sensor nodes are deployed in a planned manner in a structured WSN, where as in unstructured network the deployment of nodes is Adhoc. WSN are used in the field of military, monitoring and tracking, surveillance, natural calamities relief, health monitoring, hazardous environment, seismic monitor. The environment plays a major role in determining the size of the network, the deployment scheme, and the network topology. Restrictions on the size, cost constraints, deployment and application scenarios results in constraint on resources such as computational speed, energy, memory, and bandwidth.

The four main units of sensor node are a sensor, processor, a transceiver and a power unit. Analog to Digital Converters (ADCs) is part of sensing unit. The signal from the ADC or the digital sensor is given to the microcontroller (processing unit) to carryout computations and transmits the processed data.

Sensor networks are data centric whereas adhoc networks are address centric (information is sent based on data/ address). So the routing of information in the sensor networks is different. Because of the resource constraints in sensor networks, routing protocols used for adhoc networks cannot be directly used for WSN. The design challenges for sensor networks include.

Random sensor node deployment results in the autonomous set up and maintenance of the networks.

*Author for correspondence
Infrastructure-less nature of sensor networks demands the routing and maintenance algorithms to be distributed.

Energy is the major constraint while designing protocols and hardware, as sensors rely on battery for power, which cannot be replaced or charged.

Routing protocol should dynamically include or avoid sensor nodes in case of failure or powering up of new nodes.

The sensor network architecture is either layered or clustered. In layered architecture, layers refer to the nodes that have the same number of hop count to base station. Clustered architecture groups the nodes into clusters, managed by cluster head.

In general, wireless sensor networks communicate in a many to one pattern where data is relayed to base station from the sensor node. The application of sensor network decides the deployment of the WSN. Sensor networks are susceptible to failures because of the constraints such as battery power, memory, communication capability and deployment in the harsh and unattended environment. When routing algorithm is affected, it creates malicious attacks, which propagates false information. Attacks in sensor network, and the analysis of the attack constitutes the first part of the paper followed by the discussion of existing methodology for detecting the sinkhole attacks. One of the important issues in wireless sensor network is security. As the sensor nodes are deployed in hostile environments, networks are prone to different types of attacks. A challenging task is the designing and implementing security protocols to accommodate the limitations such as energy, storage and computational capabilities. Attacks can occur in any layer of the protocol stack in WSN. This paper is organized as follows, section 2 deals with the discussion on classification of the attacks in WSN based on OSI layering model and the attributes to analyse the severity of the attacks. Section 3 deals with the performance evaluation of the network when the system is subjected to sinkhole attack. The scenarios analysed are, varying network size number of compromised node, intruder power and the location of the sinkhole attack. Section 4 deals with survey of sinkhole detection methods and the techniques so far available for detecting the sinkhole attack is tabulated.

### 2. Attacks in Wireless Sensor Networks

Considering the extensive application opportunities, the most important aspect that requires concentration in the design of wireless sensor networks is the security issue. Active attacks modify or alter the data whereas the passive attacks try to deplete the energy resources.

The attacks can be classified based on Open System Interconnect (OSI) layering model. The physical layer, which is the basis of network operation, deals with the transmission of raw bits of information through a wired/wireless medium. Some of the functions of the physical layer include signal detection, modulation, encoding, and frequency selection. As all the upper layer functionalities depend on this layer, many attacks target the physical layer. Jamming, Tampering and eavesdropping attacks can be classified as the physical layer attacks.

#### 2.1 Jamming

By deploying enough number of jamming devices, the adversaries can prevent the communication of the sensor network over the wireless/wired medium. This technique introduces interference by jamming the carrier frequency using high energy signals such that the availability of the transmission media is disrupted. Sensors near the jamming device are prone to higher background noise which results in the easier identification of the jamming devices.

#### 2.2 Tampering

An easy method to attack is to cause damage or modify the node physically so that the services can be stopped or altered. As the base stations have the greater responsibility of communications and data processing, the impact of tampering the base station will be greater than the normal node. Due to dense deployment and more redundancy in most of the sensor networks the effectiveness of causing physical damage to a sensor is minimal. A more threatening attack, Denial of Service is possible if the sensitive data is extracted by modifying the node.

#### 2.3 Eavesdropping

The data traffic on the communication channels and the transmission is monitored by eavesdropping attacker, such that the sensitive information can then be extracted by analysing the collected data. As the mode of communication by the sensor node is wireless transmission, i.e. signals are broadcast; the attackers can obtain raw data by plugging themselves into the wireless channel. The severity depends on the power of antenna and such attacks are rarely detectable. Cryptography and access restriction techniques such as Sleeping, hibernating, use of
directional antenna can reduce the occurrence of attack in the physical layer.

The right for information transmission through the channel over a certain period of time is achieved by the wireless MAC protocols, which controls the exchange of control packets. Malicious nodes disobey the coordination rules based on MAC protocols to create packet collision by interrupting the traffic. The MAC layer identification is forged and created identity spoofing or Sybil attack. Misbehaving detection is identified by watchdog, game theory approach. Radio resource testing can be done to avoid Sybil attack. Position verification, code attestation, sequence checking, identity key association helps to reduce false identification.

The key issue in the network layer is to find the optimal path to the destination. Adversaries gain access over the routing path and redirect the information and distribute false routing direction or launch Denial of Service attack. Overflowing of routing tables, poisoning routing tables and caches creates false routing attack.\(^6\)

Replication of packet creates flooding attack which consumes both the sensor node power and the bandwidth of the network. In black hole attack the attacker drops or swallows all the information decreasing the throughput of the neighbouring node. The harm created by the blackhole attack depends on the location of the attacker node. Adversaries close to the base station creates more severity than at edge of the network. The attacker conveys a false optimal path by a method of announcing more power, bandwidth or better route such that the malicious node attracts traffic from a certain region and either drops or selectively forwards the information. Two or more adversaries create a tunnel and advertises the shortest path with greater communication resources such as power and bandwidth which results in the formation of wormhole attack. Restricting the routing access, detecting the false routing and detection of wormhole attack by using synchronized clock, directional antennas, multidimensional scaling are the countermeasures for network layer attacks.

Application layer incorporates the services seen by the users such as data aggregation and time synchronization of clocks for co-operative operation. An attack in this layer manipulates and creates false data resulting in abnormal actions. Clock skewing attack, skew the sensor clock and disseminates false timing information. Selective message forwarding and data aggregation distortion are attacks common in this layer. The countermeasures are data integrity protection and confidentiality protection.

The cross layer attacks and the intra layer attacks demands further research and countermeasures. Attacks in various layers in tabulated in Table 1 and 2 lists the attributes which can be analyzed to check the severity of the attacks.

In general intrusions are categorized into two methods, misuse IDS or signature based detection and anomaly IDS. The attack patterns called signatures are predefined in misuse based whereas the normal behaviour is defined in anomaly detection. The normal behaviour of node can be characterized through its attributes\(^7\). It is obvious that the anomaly detection is more advantageous as

**Table 1. Attacks in various layers**

| Layer            | Attacks                                      |
|------------------|----------------------------------------------|
| Physical layer   | Jamming attacks , Tampering attacks, eavesdropping |
| Data link layer  | Jamming, Collision, exhaustion               |
| Network layers   | Spoofing or replaying information, Selective forwarding or black holes, Sink holes, Wormholes, Sybil attacks, Node replication attacks, Hello flood , Attacks against privacy |
| Transport layer  | Flooding, Injects false messages, Energy drain attacks |
| Application layer| Attacks on reliability                      |

**Table 2. Attributes for the attacks**

| Attacks          | Attributes                                      |
|------------------|-------------------------------------------------|
| Sinkhole attack  | Packet receiving rate. Hop count, Packet forward rate, RSSI, Packet arrival process |
| Blackhole attack | Packet dropping rate, Packet arrival process    |
| Wormhole attack  | Signal power/ received signal strength, Transmission power/packet sending power |
| Selective forward attack | Signal power/ received signal strength, Transmission power/packet sending power |
| Hello flood attack | Packet dropping rate, Packet arrival process, Packet forward rate, Forward delay time |
| Jamming attack   | Signal power/ received signal strength, Transmission power/packet sending power |
| Sybil attack     | Packer sending rate                             |
|                  | Node density                                    |
new, undefined attack pattern can also be recognized. Routing protocols in sensor networks are simple when compared to adhoc networks which make the sensor network more vulnerable to different kinds of attack. It is difficult to develop a common mechanism that can detect all attacks as each attack has its own characteristics and nature. Performance of the adhoc network is analysed with respect to various parameters\(^{20}\).

### 3. Performance Evaluation of Sink Hole Attack

Malicious nodes in the network either drop or selectively forward the traffic packets\(^3\). In general sinkhole attacks are implemented by varying the parameters with respect to routing algorithms. Intruder attracts the surrounding nodes with fake routing information, and then either modifies or selectively forwards the information. The sinkhole attack prevents the base station from obtaining exact and complete sensed information, thereby causing serious threat and also enables other attacks such as selective forwarding and wormhole. Sinkhole can be implemented by modifying any of the routing protocol such as AODV or tree based routing.

Tree based routing topology initiated and created by sink for the layered architecture\(^4\) is the most applied routing protocol, whereas LEACH is for clustered architecture. In this simulation tree based routing protocol is implemented for data transfer. Routing topology is built from the sink by advertising the hop count information. Sinkhole attack, the attacker node pretends as though it is closer to the base station than its entire neighbour. When the data packets are routed the few packets are dropped and it selectively forwards the information.

#### 3.1 Simulation Results

A network is created with static sensor nodes and a base station located in a remote area. All the nodes are capable of wirelessly communicating with its neighbour nodes that are in its transmission range. The data is routed to the sink from the sensor node by means of tree based routing topology where a tree is routed at the sink. The routing tree is an aggregation of shortest paths from sensor to the base station based on a cost metrics, such as hop count, loss or delay\(^8\). In this simulation the routing tree is built based on the hop count distance parameter. The routing topology is refreshed regularly through routing messages.

Simulations are performed in NS2 to analyze and evaluate the effect of sinkhole attacks in various scenarios. The sensor field includes a base station and sensor nodes. To measure the performance of the system when subjected to sinkhole attack based on tree based routing protocol, we analyze the parameters of the network without attack and with sinkhole attack. The network is simulated with 100 nodes the effect of parameters due to the presence of 2 malicious nodes is tabulated in Table 3.

Table 3 it is analyzed that, there is a decrease in the performance due to malicious nodes, as the number of packets received reduces, PDR also reduces. Due to the presence of attacker, the delay reduces as the attacker advertises the shortest route to the destination. Throughput, which represents the rate of successful delivery of data packet decreases and the jitter increases due to attack. Total and average energy consumed decreases in the presence of attack.

After analyzing the network due to the presence of attacker, the variation of the parameter is analyzed based on the different characteristics of compromised topology (attack scenario), i.e. by varying: 1. Network size, 2. The number of malicious nodes in the network, 3. Varying the intruder power, and 4. Location of compromised node. The performance parameters of the network such as packet delivery ratio, throughput and average energy consumption are analyzed. Packet delivery ratio represents the number of received data packets with respect to the count of data packets sent by a source node. Throughput is the rate of data packets delivered successfully. Table 4 illustrates the simulation parameters for various scenarios.

#### 3.1.1 Scenario 1: Varying the Network Scale

In this section the performance of the network is analysed with reference to the network scale. We analyse the constant area network and constant density network i.e
Table 4. Simulation parameters for various scenarios

| Scenario Parameter | Varying size | Varying No. of malicious nodes | Varying Intruder power | Location of malicious nodes |
|--------------------|--------------|-------------------------------|------------------------|-----------------------------|
| Number of nodes    | 50,75,100    | 100                           | 100                    | 100                         |
| Size of the network| 100x100, 150x150, 200x200 | 100x100 | 100x100 | 100x100 |
| Initial energy     | 100 J        | 100 J                         | 100 J                  | 100 J                       |
| Number of malicious nodes | 2          | 2                             | 0,1,2,5                | 2                           |

1) density is increased by keeping the area constant and 2) density is increased in proportional to the area. The density of the network is increased from 50 to 75 and 100 nodes. This scenario is analyzed by keeping the deployment area as constant (100x100) and the area is increased, (150x150, 200x200) when the density is increased (number of nodes: 75,100). The performance parameters i.e. packet delivery ratio, throughput, and average energy consumption are analyzed and the three parameters are shown in Figure 1 and 2 for the network with constant area and area proportionally increased for the increase in the density. From the figure it is analysed that when the sensors are close to each other the packet delivery ratio and the number of packets successfully transmitted are better when compared to the network where they are placed apart. The performance degrades due to the presence of malicious nodes.

For the constant density compromised network, when number of nodes increases, the packet delivery ratio and the throughput is less, as a result it is observed from Figure 3 such that the average energy consumed by the network is less when it is compared to the constant area compromised network.

3.1.2 Scenario 2: Varying the Number of Malicious Nodes in the Network

In this scenario the variation of the malicious node is simulated to analyse the effect of performance of the network.
Sinkhole Attack in Wireless Sensor Networks: Performance Analysis and Detection Methods

Figure 3. Average energy consumption.

single and multiple malicious nodes. Figure 4-6 shows that the packet delivery ratio, throughput and the average energy consumed exponentially reduces as the attacker nodes increases in the network. The performance of the network is degraded.

3.1.3 Scenario 3: Varying the Intruder Power

The network is simulated with 2 malicious nodes, initial energy to be 100J. The parameters are analyzed by considering the power of the intruder to be the same as that of the other nodes. Then the simulation is carried out with the energy of the malicious nodes to be 150 J and the energy of all other nodes to be 100J. As the routing is based on tree based routing topology, it is observed that the effect of the parameters remains the same with increase in the energy of the malicious nodes. I.e. there is a same proportion of degradation in packet delivery ratio, throughput and average energy consumed though the power of the intruder is high. The life of the malicious node is increased when it has more power compared to the other nodes. There will definitely be effect on the parameter if the routing is based on the energy.

3.1.4 Scenario 4: Location of Compromised Node

The distribution of the malicious node definitely has an impact on the extent of damage. The network is analyzed when the sinkhole is near and far away from the base station. The effect of the attack is higher when the compromised nodes are near the sink because these nodes

Figure 4. Packet delivery ratio.

Figure 5. Throughput.

Figure 6. Avg. Energy consumption – increase in no. of malicious node.
receive and in-turn drop more data than the other malicious nodes that are farther away.

4. Survey of Sinkhole Attack Detection Mechanism

This section deals with the various solutions based on the survey for detecting the sinkhole attacks in wireless sensor networks. Received Signal Strength Indicator (RSSI) parameter detects the sinkhole attack\(^9\), which includes Extra Monitor (EM) nodes, other than the normal nodes which finds the position of nodes. The communication range of EM is greater than the normal nodes. It is a centralized approach where the extra monitor nodes will receive the message and the RSSI value whenever any node sends the message to the network. The EM nodes send this information to the base station, the flow of the received message is compared with the normal flow and the attack is detected based on the visual graphic map. Data consistency of the nodes are monitored for abnormal behavior detection\(^11\). If the nodes behavior exceeds a threshold value, it is identified as malicious. Base station identifies the malicious node after analyzing the routing pattern. Various detection mechanisms are tabulated in Table 5.

5. Conclusion

Various attacks in different layers are discussed in this paper. Performance of the system is analyzed when the network is subjected to sinkhole attack. Different scenarios are simulated by varying the size of the network, number of malicious node, intruder power and the location of the sinkhole attack. Parameters such as average energy consumption, throughput and packet delivery ratio are analyzed. It is seen that the network performance is degraded by the implementation of the attack and there is a decrease in parameters analyzed when subjected to various scenarios. It is concluded that for the scenario with same number of attacker nodes, the networks with greater number of nodes has less danger than the sparse network, performance reduces as the number of malicious nodes increases, the life of the adversary node is increased when it has more power compared to the other nodes and the effect of attack is higher when the compromised nodes are near the sink. Finally various techniques available for detecting the sinkhole attack are tabulated.

6. References

1. Akyildiz IF, Su W, Sankarasubramaniam E, Cayirci C. Wireless Sensor Networks: A Survey, Computer Networks, Elsevier. 2002; 38(4):394–422.
2. Murthy CSR, Manoj RS. Ad Hoc Wireless Networks: Architectures and Protocols by C. Siva Ram Murthy, Prentice Hall, 2004.
3. Ye F, Chen A, Lu S, Zhang L. A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks. In: Conference on Computer Communications and Networks, Arizona, USA, Scottsdale, AZ. 2001; p. 304–09.
4. Cetintemel U, Flinders A, Sun Y. Power-Efficient Data Dissemination in Wireless Sensor Networks, In: ACM MobiDE. San Diego, CA, USA. 2003; p. 1–8. Crossref
5. Sen JA. Survey on Wireless Sensor Network Security, International Journal of Communication Networks and Information Security (IJCNIS). 2009; 1(3):55–78.
6. Xing K, Srinivasan SSR, Rivera M, Li J, Cheng C. Attacks and Countermeasures in Sensor Networks: A Survey Network. Security Springer, 2005, p. 251–72.

Table 5. Detection mechanism.

| Author            | Detection mechanism                                             |
|-------------------|-----------------------------------------------------------------|
| Tumrongwittayapak | RSSI values from extra monitor (EM) nodes                       |
| Edith11           | Analyzing data consistency and network flow information         |
| Daniel Dallas12   | Hop count monitoring                                           |
| Sheela13          | Mobile agent based approach                                    |
| S.Roy14           | Message digest algorithm                                       |
| Choi16            | Dynamic trust management system                                 |
| Villapando17      | Distributed network coding                                     |
| Krontis18         | Rule based detection on Minroute and Multihop LQI protocol      |
| Shafei19          | Geo-statistical sampling based on energy expenditure             |
| Liu20             | Swarm intelligence                                             |
| Sreelaja21        | Ant colony optimization attack detection                        |
| Krontis22         | Rule based voting method                                       |
| Changlong23       | CPU usage                                                      |
| Fang-Jiao Zhang24 | Redundancy mechanism                                           |
| Shamshirband25    | Density based fuzzy logic algorithm                             |
7. Joseph C, Kishoreraja PC, Baskar R, Reji M. Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios, Indian Journal of Science and Technology. 2015; 8(25):1−10. Crossref
8. Reji M, Raja PCK, Joseph C, Baskar R. Performance Metrics of Wormhole Detection using Path Tracing Algorithm, Indian Journal of Science and Technology., 2015; 8(17):1−9. Crossref
9. Fessent FL, Ppadimitriou A, Viana AC, Sengul C, Palomar P. A Sinkhole Resilient Protocol for Wireless Sensor Networks: Performance and Security Analysis, Computer Communications. 2012; 35(2):234–48.
10. Tumrongwitayapak T, Varakulsiripunth R. Detecting Sinkhole Attacks in Wireless Sensor Networks ICROS-SICE International Joint Conference, Fukuoka International Congress Center, Japan; 2009. p. 1966–71.
11. Edith CH, Ngai N, Liu JB, Michael R, Lyu L. An Efficient Intruder Detection Algorithm Against Sinkhole Attacks in Wireless Sensor Networks, Computer Communications. 2007; 30(11-12):2353–64. Crossref
12. Dallas D, Leckie C, Ramamohana Rao K. Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks. 15th IEEE International Conference on Networks, ICON Adelaide, SA; 2007. p. 176–81.
13. Sheela D, Kumar N, Mahadevan CG. A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks. IEEE-International Conference on Recent Trends in Information Technology, ICERTIT, Chennai, Tamil Nadu; 2011. p. 527–32.
14. Sharmila S, Umamaheswari G. Detection of Sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms. International Conference on Process Automation, Control and Computing (PACC) Coimbatore; 2011. p. 1–6.
15. Roy S, Singh S, Choudry S, Debnath N. Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management, Proceedings of IEEE Symposium on Computers and Communnication, Marrakech; 2008. p. 537–42.
16. Choi B, Cho Kim J, Hong C, Kim J. A Sinkhole Attack Detection Mechanism for LQI Based Mesh Routing in WSN, Proceedings of International Conference on Information and Networking, Chiang Mai; 2009. p. 1–5.
17. Villaipando R, Vargas C, Mnoz D. Network Coding for Detection and Defence of Sinkhole Attacks in Wireless Reconfigurable Networks. Proceedings of International Conference on Systems and Network Communications, Cancun; 2008. p. 286–91.
18. Krontis I, Giannetos T, Dimitriou T, Mpasoukos M. Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side. Proceedings of IEEE International Conference on Wireless and Mobile Computing, Avignon; 2008. p. 526–31.
19. Shafei H, khonsari A, Drakshi H, Mousavi P. Detection and Mitigation of Sinkhole Attacks in Wireless Sensor Networks, Journal of Computer and System Sciences. 2013; 80(3):644–53. Crossref
20. Liu Y, Passino KM, Intelligence S. Literature Overview, Department of Electrical Engineering. The Ohio State University, 2000.
21. Sreelaja NK, Pai GAV, Swam S. Intelligence Based Approach for Sinkhole Attack Detection in Wireless Sensor Networks, Applied Soft Computing. 2014: 19:68–79. Crossref
22. Krontis I, Giannetos T, Dimitriou T. LIDeA: a Distributed Lightweight Intrusion Detection Architecture for Sensor Networks. Proceedings of ACM Secure Communications, NY; 2008.
23. Chen C, Song M, Hsieh G. Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks. IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), Beijing, China; 2010. p. 711–16. PMCid:PMC3398139.
24. Sinkhole S. Attack Detection Based on Redundancy Mechanism in Wireless Sensor Networks, Fang-Jiao Zhaa, Li-Dong Zhai, Jn-Cui Yangb, Xiang Cuic, Procedia Computer Science. 2014; 13(31):711–20.
25. Shamshirband S, Amini A, Anuar NB, Kiah MLM, Wah Y. Steven Furnell D-FICCA: A Density-Based Fuzzy Imperialist Competitive Clustering Algorithm for Intrusion Detection in Wireless Sensor Networks, Measurement. 2014; 55:212–22. Crossref
26. Kishore Raja PC, Sathishkumar M, Christeena Joseph, Reji M, Radhika Baskar. Real Time Experimental Analysis of Mobile Ad-Hoc Traffic in Indoor and Outdoor Environment, International Journal of Engineering and Technology. 2015 Jun-Jul; 7(3):922–28.