2012 IACSIT Hong Kong Conferences
IPCSIT vol. 30 (2012) © (2012) IACSIT Press, Singapore

Wireless Sensor Networks: Attack Models and Detection

Vinod Kumar Jatav, Meenakshi Tripathi [+], M S Gaur and Vijay Laxmi

Department of Computer Engineering, Malviya National Institute of technology, Jaipur, Rajasthan, India

Abstract Unattended installation of sensor nodes (Motes) in the environment causes many security threats in the wireless sensor networks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station [2]. Routing protocol MintRoute is used to implement this attack. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as, forwarding only the selective packets i. e. selective forwarding or dropping all the packets and forming a blackhole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. This paper presents a mechanism to launch sinkhole attack based attacks such as selective forwarding and balckhole attack in wireless sensor networks. The proposed work includes detection and countermeasure rules to make the sensor network secure from these attacks. It is observed through simulation that our proposed methods for detection and countermeasure achieve high degree of security with negligible overheads.

Keywords: wireless sensor network, security attack, adversary node, legitimate node.

1. Introduction

Wireless sensor networks are network of thousands of sensor nodes (Motes). Sensor nodes are small in size, cheaper in price with restricted energy storage, less memory space and limited processing capability. Like all other wireless networks, remote wireless sensor networks are also vulnerable to many security threats. Unreliable communication and unattended installation of sensor nodes, increases difficulty in making the existing network security countermeasures efficient for these networks. The memory space and power restrictions of sensor nodes also make it difficult to implement traditional security solutions. So these networks require some unique security policies.

The aim of this paper is to make sensor network secure from various routing attacks such as sinkhole attack, selective forwarding attack and blackhole attack on MintRoute routing protocol.Once sinkhole attack is implemented, it is easy to implement selective forwarding and blackhole attack using sinkhole attack. Selective forwarding and blackhole attacks are very disastrous attacks for sensor networks if used with sinkhole attack because the intruder can drop most of the important packets. After implementation of these attacks, we designed detection rules and countermeasure techniques for all these attacks.

Section 2 describes the proposed work in detail. It covers the design issues of sinkhole attack, selective forwarding attack and blackhole attack, their detection rules and countermeasures. Section 3 highlights the simulation of various attacks and results. Section 4 concludes the paper.

2. Proposed Work

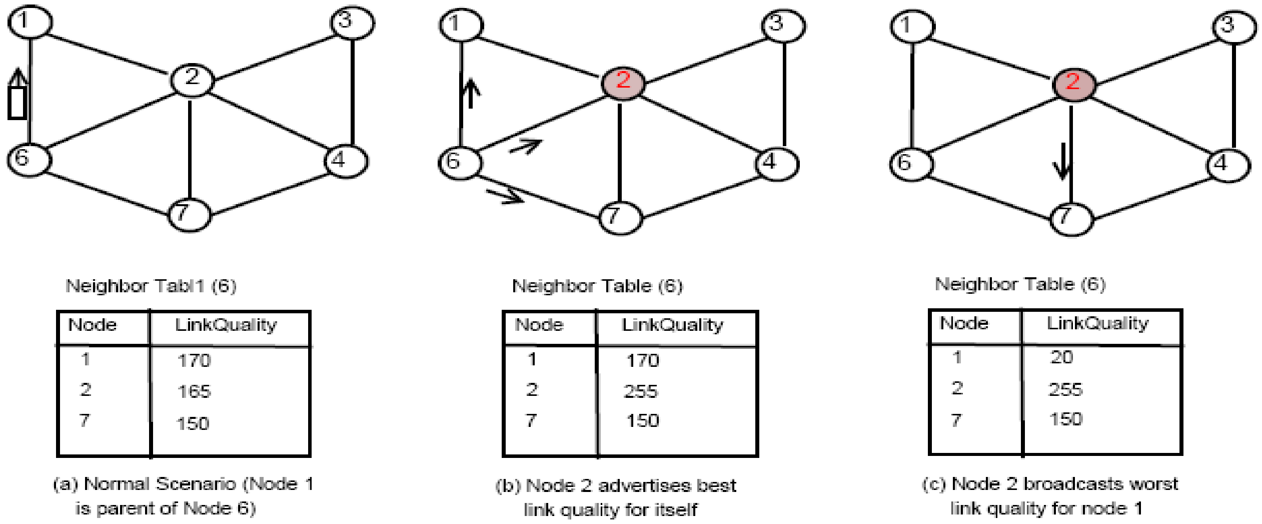
Selective forwarding and blackhole attacks are hard to detect if launched using the sinkhole attack. This part of paper shows detailed design aspects of launching and detecting sinkhole, selective forwarding and balckhole attack with their countermeasures [2][3].

[+] Corresponding author. Tel.: + 91-141-2713419; fax: +91-141-2529154.
E-mail address: *indian.meenakshi@gmail.com.*

2.1. Implementation of sinkhole attack

Routing protocols, such as MintRoute make the use of estimated link quality to maintain the routing tree. The adversary node which is one of the compromised nodes in the network launches sinkhole attack and forces the neighboring nodes to make itself as their parents rather than current parent. MintRoute protocol follows the estimates of link quality as major parameter for changing the current parent. This protocol is robust enough and does not allow parent changing process until and unless there is not a valid reason. Sinkhole attack can be launched using two steps on MintRuote: *first,* the attacker node advertises a better link quality (near 255) for itself and then in *second step,* it changes the link quality of current parent to worst value. This way the attacker triggers parent changing mechanism in their children and adversary node . Now the adversary node will work as a sinkhole node.

The adversary node (sinkhole node) snoops the route update messages from its neighbors, modifies the link estimates in them and sends back to the neighbors as their actual sender of the message. The occurrence of sinkhole attack is shown in the Figure 1 below.



Neighbor Tabl1 (6)

Node	LinkQuality
1	170
2	165
7	150

(a) Normal Scenario (Node 1 is parent of Node 6)

Neighbor Table (6)

Node	LinkQuality
1	170
2	255
7	150

(b) Node 2 advertises best link quality for itself

Neighbor Table (6)

Node	LinkQuality
1	20
2	255
7	150

(c) Node 2 broadcasts worst link quality for node 1

Fig. 1: Sinkhole attack on MintRoute

Here, sensor node 2 is an adversary node. Current parent of node 6 is sensor node 1 in this scenario. Adversary node 2 advertises a false link quality estimate (255) to itself in the network. But to change the current parent only better link quality for itself is not sufficient. So, whenever attacker receives the route update packet of node 6, it changes the link quality of node 1 to a low value (i.e. 20) and sends it back to 6 as a unicast packet, impersonating 1. Here node 6 thinks that the route update packet is sent by node 1. Node 6 estimates the link quality and refreshes own neighbor table with the new entry. This way node 6 triggers the parent changing mechanism and chooses node 2 as new parent. Hence the node 2 becomes the new parent of the node 6. The same process can be applied to most of the other neighbors of node 2 so that for all neighbors node 2 becomes their parent and hence receives most of the traffic i.e. it becomes a sinkhole node.

2.2. Detection of sinkhole attack

We are aware that the data flow in wireless sensor networks takes place in wireless communication media (air). Hence the sensor nodes are free to snoop the data flow in the network and can receive or analyze individual data passing from their immediate neighbors. On this basis this section talks about the detection rules for sinkhole attack. Figure 2(a) shows normal behavior of a 10 node wireless sensor network. In figure 2(b) attacker node 2 implements sinkhole attack in the network and manages to attract most or all of the traffic. Node 1 and 3 are near to base station and forwards packets to it. But sinkhole attack forces these two nodes to forward their packets to attacker node 2. Whenever an adversary node tries to cheat any other node in the sensor network, the following detection mechanism triggers. The main idea is that the sensor nodes should receive route update packets from the original sender node.

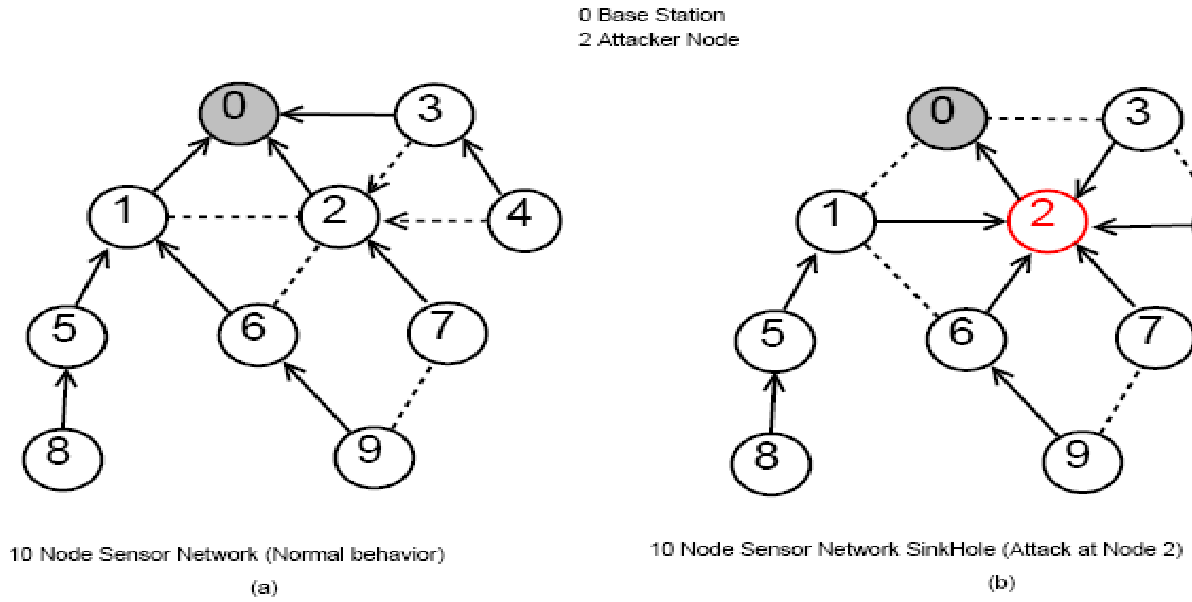

0 Base Station
2 Attacker Node
0
1
2
3
4
5
6
7
8
9
10 Node Sensor Network (Normal behavior)
(a)
10 Node Sensor Network SinkHole (Attack at Node 2)
(b)

Fig. 2: Two phases of 10 Node Sensor Network

There are two rules to detect the attack: According to first rule the route update packet should be originated by one hop neighbor only. Route update packet consists of sender node ID and link estimates of the node. For example given in Figure 2 when rule 1 is triggered at node 1 it overhears the rout update packet which is sent by attacker node 2 impersonating node 1. Node 3, 4 and 7 will also realize that they are update packets from node 1 which is not a one hop neighbor.

Second rule is based on the anomaly detection. In MintRoute protocol, sensor nodes calculate the estimate for link quality for their neighbors. Nodes also receive link quality estimates from neighbor with the help of route update packets. There may not be a big difference in these two estimates of link quality. If the link quality estimate is showing a deviation of value more than 50, then it may be an impersonated value [3].By applying both the rules together we can detect the sinkhole node.

2.3. Selective forwarding attack using sinkhole attack

Selective forwarding attack can be implemented using sinkhole attack. After the establishment of routing tree in sensor network, an adversary node may cause the dropping or forwarding of selected packets. We have implemented two types selective forwarding attack, time interval based and node id based attack.

- Time Interval based attack: The adversary node can make the use of time interval to drop or forward the packets received. Each simulation time consists of time interval for which the adversary launches the selective forwarding attack. This may cause the loss of important information. In some critical application like military surveillance selective forwarding attack is more harmful, as movements of opposing forces may not be reported for the given interval.
- Node ID based attack**:** Another way to implement the selective forwarding attack is based on the packet node id. Each packet consists of the node ID of originating sensor node, which is a unique identification number in the network. The adversary node can drop or forward the selected packets with specific node id. This selection of node id is generated using a random function of node Ids. So the proper and complete information from the sensor nodes is not being received by the base station. The base station will not be aware of this selective drop of the packets, as it is receiving the packets in regular fashion.

Detection of selective forwarding Attack

Adversary node starts to drop some important packets in the selective forwarding attack. So the sink (base station) is not able to receive all the packets destined to it from sender nodes. The detection of selective forwarding attack depends upon the total number of packets sent from the sensor nodes to the sink. There may be chance of packet drops due to congestion also, but if the drop ratio increases by threshold value then it is one of the conditions of selective forwarding attack.

Countermeasures of selective forwarding attack

Once the attacker node is detected in the network. An alternate route can be found through which packets can be routed thus, keeping the loss of packets under control. Whenever the attacker uses time interval for packet dropping, the neighbor nodes change their parent and thus traffic route can be changed.

2.4. Blackhole attack using sinkhole attack

Once the routing tree has been established for the whole sensor network and an adversary node generates a sinkhole, most of the traffic is forced to flow through adversary node. Now the adversary node broadcasts a 0 metric for all neighbors causing them to route packets towards it and then it drops all the received packets instead of forwarding them. Like this a blackhole is created.

Detection of blackhole attack

To detect the blackhole attack in sensor network the watchdogs are used. The watchdogs are able to analyze the misbehavior of adversary node. Whenever the amount of packet drops reaches to a specific value (threshold value) these watchdog alert the network about it. They maintain a buffer to store the information of packets not being forwarded in the network within a fixed period of time. So the detection of blackhole attack is possible by watchdog's observation.

Countermeasures of blackhole attack

Once the watchdogs have detected the attacker in the network, an alternate route is found through which packets can be routed. This way it is possible to keep the loss of packets under control. Once the neighbor nodes have detected the adversary node, they can change their parent. Hence the traffic flow has been changed and the adversary node does not receive the packets.

3. Simulation

TinyOS is used to implement the proposed work and source code is written in programming language NeSC on TinyOS. The simulation of sinkhole attack is completed on TOSSIM simulator with 3, 5, 10, 20 and 40 sensor nodes. Simulation time ranges from 100 mili seconds to 10000 mili seconds. Packet size has been fixed to 36 bytes with the payload of 29 bytes. Example topology for simulation is shown in Figure 2. Node 0 is the base station and node 2 is used as attacker node. The routing tree has been created using two way link quality estimates between source and destination nodes according to MintRoute.

Figure 3 shows the result of sinkhole attack on 10 node network, where simulation time is 500 mili seconds. The received packets at attacker node 0 decreases as the attacker node 2 attracts the traffic flow of node 1 and 2 towards itself.

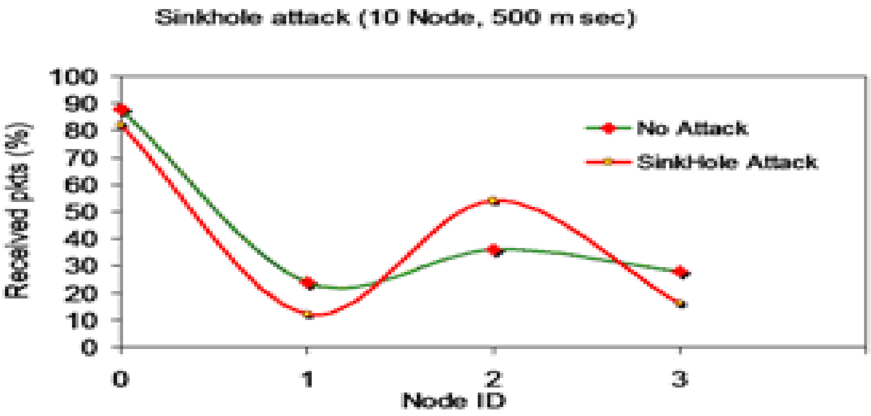


Fig. 4: Sinkhole attack

Once Sinkhole attack has been implemented, node ID 2 will work as an adversary node in the network. Figure 4 (a) and 4 (b) shows the result of selective forwarding attack using sinkhole attack based on time interval and packet node ID. Figure 5 shows that after using the countermeasure technique, dropping of packets is decreased and the total received packets at node 0 has increased.

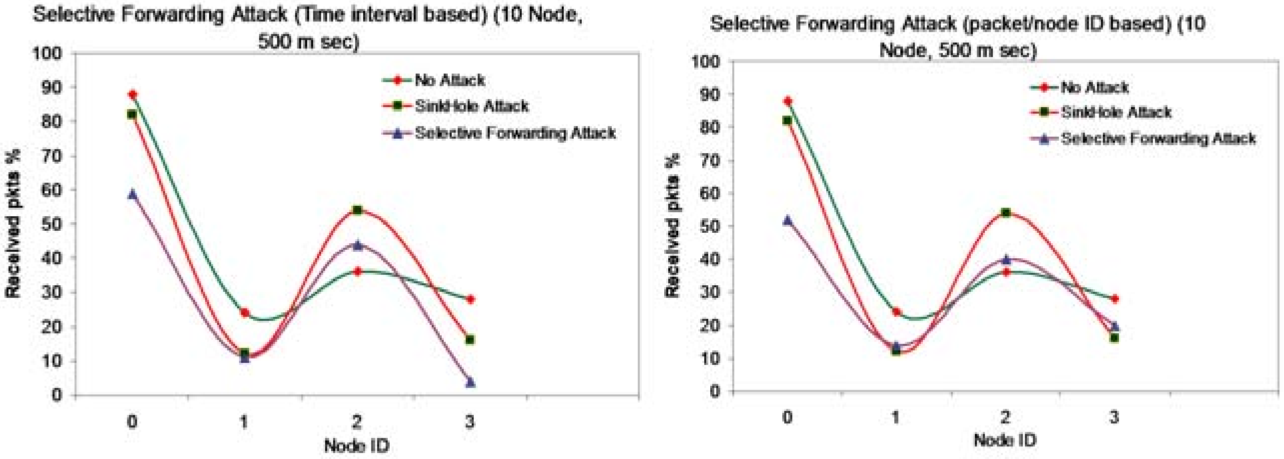


Fig. 5: Selective Forwarding attack using Sinkhole (a) Time interval based (b) Packet/Node ID based

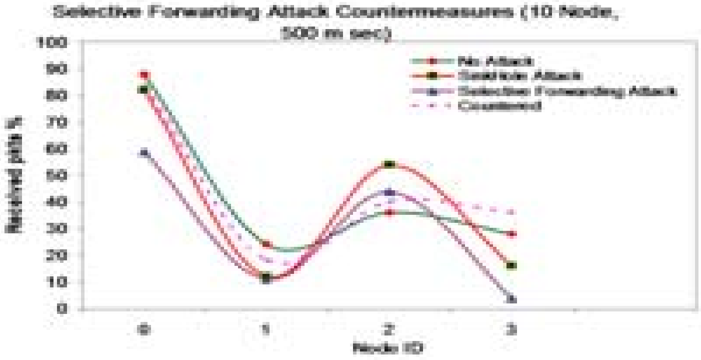


Fig. 6: Countermeasure for Selective Forwarding attack

Results for blackhole attack using sinkhole attack are shown in Figure 7(a). From Figure 7 (b) it is clear that the percentage of received packets has been increased at base station and packets received at node 2 have been decreased drastically. It shows that the effect of blackhole attack is weakened.

Figure 8 (a) analyzes the comparisons between all three attacks implemented. Here we can see that selective forwarding and blackhole attack are more vulnerable to sensor networks if these are implemented using sinkhole attack. The no. of packet drops is more in this case. Figure 8 (b) shows the comparisons between countermeasure techniques for all three attacks implemented. Here we can see that countermeasures for blackhole attack show better results. The number of packet drop is much less in this case.

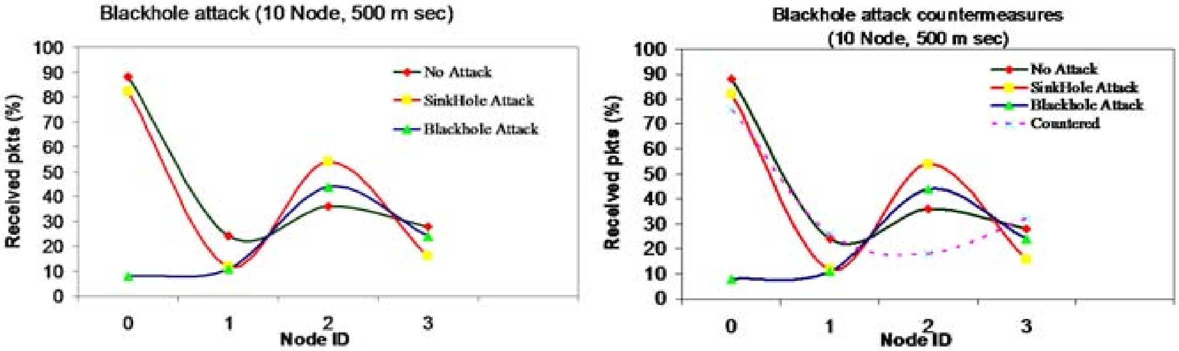


Fig. 7: Blackhole attack using Sinkhole (a) Attack (b) Countermeasure

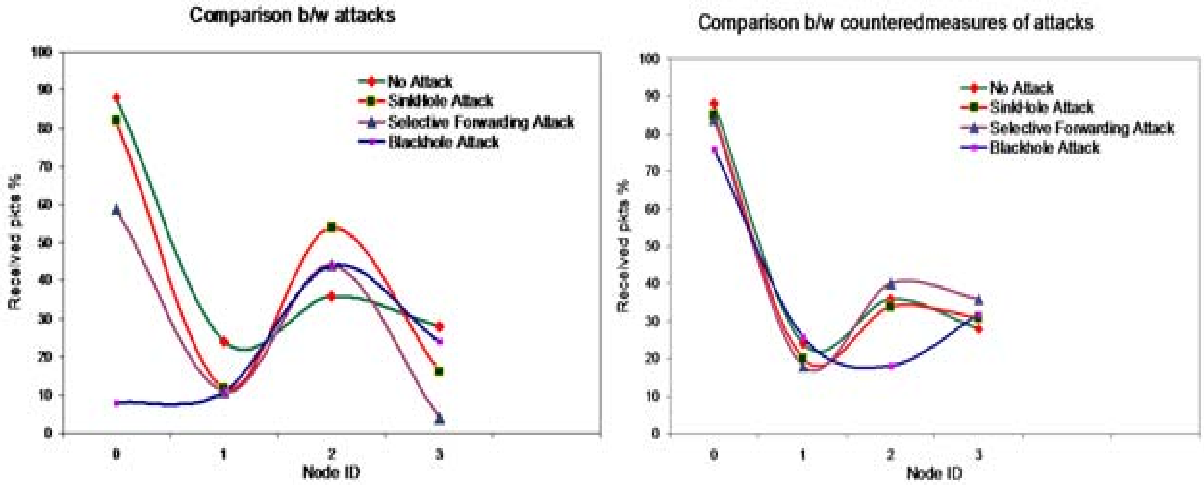


Fig. 8: Comparison (a) Attacks (b) Countermeasures

4 Conclusion

The paper is all about implementation and detection of routing security attacks in wireless sensor networks. The paper includes implementation of sinkhole attack on MintRoute protocol in wireless sensor networks. The sinkhole attack is used to launch selective forwarding attack and blackhole attack. Simulation results show that these attacks are more severe if implemented using sinkhole attack. The number of packets received at base station decreases exponentially. Proposed detection rules and countermeasures help to make the network secure against these attacks. In future by creating tunnel between two attacker nodes on the basis of link estimates, wormhole attack may also be implemented.

5. References

[1] C. Karlof and D. Wagner. “Secure routing in wireless sensor networks: Attacks and countermeasures” *AdHoc Networks Journal*, vol. 1, pp. 293-315 , September 2003.

[2] I.Krontiris, Thanassis Giannetsos, Tassos Dimitriou. “Launching a Sinkhole Attack in Wireless Sensor Networks” in *Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communication,(wimob),* 2008.

[3] I.Krontiris, Thanassis Giannetsos, Tassos Dimitriou. “Intrusion detection of sinkhole attacks in wireless sensor networks” in *Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors 07)*, Wroclaw, Poland, July 2007.

[4] E. C. H. Ngai, J. Liu, and M. R. Lyu. “On the intruder detection for sinkhole attack in wireless sensor networks” in *Proceedings of the IEEE International Conference on Communications (ICC 06)*, Istanbul, Turkey, June 2006.

[5] A.Woo, T.Tong, and D.Culler. “Taming the Underlying Challenges of Reliable Multihop Routing in WSNs” CM *Sensys 2003*, Los Angeles, November 2003.

[6] Liping Teng, Yongping Zhang. “SeRA: A Secure Routing algorithm Against Sinkhole Attack for WSNs” in *Second International Conference on Computer and Simulation*, 2010.

[7] C. Tumrongwittayapak and R. Varakulsiripunth. “Detecting Sinkhole Attacks in Wireless Sensor Networks” in *Communication of the ACM*, vol. 47, no. 6, pp. 53-57 , 2004.

[8] B. Yu, B. Xiao. “Detecting selective forwarding attacks in wireless sensor networks” in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (SSN2006 workshop)*,. Rhodes, Greece, pp. 18, April 2006.

[9] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. “An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks” In *TENCON 2007 - 2007 IEEE Region 10 Conference*, pages 1-4, 30, Nov.2 2007.

[10] TinyOS, http:// www.tinyos.net/ tinyos-2.x/ apps/ tests/ TestNetwork/ 2008.