International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Clone attack detection in Wireless Sensor Networks using ASP Protocol

S. Raja Rajeswari [1]; Dr. V.Seenivasagam[2] & D.Karthiga[3]

[1]Department of Computer Science and Engineering, Regional Centre of Anna University, Tirunelveli, TamilNadu 627007, India, [1]s.rajarajeswari1@gmail.com

[2]Professor, Department of Computer Science and Engineering, National EngineeringCollege (Autonomous), Kovilpatti, TamilNadu 628503, India

[3]PG Scholar, Department of Computer Science and Engineering, Regional Centre of Anna University, Tirunelveli, TamilNadu 627007, India

Abstract—

Wireless sensor networks (WSNs) are employed in harsh environments where physically no protection can be given to all nodes, so there is a chance where the intruder can capture lonely nodes and transfer all the confidential information to some other generic nodes. Using this information, the intruder can replicate the captured node in large numbers and introduce clones in the network. These cloned nodes can induce large number of attacks. Various protocols have been previously proposed to resolve this attack but they grasp large amount of resources. To overcome the clone attack, a protocol namely Area Splitting Protocol (ASP) is proposed which makes use of the restricted resources only.

***Keywords*--**Wireless Sensor Network; Clone Attack; Node Replication Attack

I. INTRODUCTION

Wireless Sensor networks are spatially distributed sensors used to monitor conditions at different locations, such as pressure, temperature, sound, vibration, motion or pollutants. WSNs are used in variety of applications like temperature, humidity, vehicular movement, pressure, noise levels, constant monitoring, forest fire, military, battlefield surveillance, flood detection, home appliances, habitat exploration of animals, patient monitoring.

WSN can be deployed in harsh and hostile environment like military and civil applications. The dense deployment of disposable, low-cost sensor nodes makes it suitable for battlefields because destruction of some nodes by hostile actions does not affect the military operations. The sensor network design is influenced by many factors, such as fault tolerance, scalability, production cost, operating environment, sensor network topology, hardware constraints, transmission media, and power consumption. Most of the sensor nodes in WSN are unshielded as tamper resistance was expensive. Thus an intruder can easily attack, analyze, clone the unshielded sensor nodes, create replicas and insert them into the network. This leads to large class of insider attacks. An intruder may replicate captured sensors and employ them into the network to launch a variety of insider attacks. This attack is referred to as clone attack [11]. Cloned nodes behave and operate in the same way as the normal nodes in the network.

In this paper ASP protocol is proposed to detect the clone attacks in WSN and it is proved that our protocol does meets all the requirements. Finally, extensive simulations of ASP shows that it is highly efficient in terms of communication overhead, memory overhead, and computation overhead and also shows improved attack

detection probability when compared to other distributed protocols.

II. RELATED WORK

Several techniques have been previously proposed to detect the clone attacks [7], [8], [9], [10]. Though they detect the clones and its replicas they absorb too much resource. Some of the techniques are discussed below.

One of the first solutions for the detection of clone attacks relies on a centralized base station [6] which collects data from nodes through multi-hops. The self- positioning mechanism is used to determine the position of sensor nodes among all N resource constrained sensor nodes when they are deployed. The basic knowledge on superimposed s-disjunctive codes is introduced, based on which we can retrieve the social community information and create a fingerprint for each sensor. Such fingerprints can help to detect clone attacks. The detection scheme consists of two phases: computing a fingerprint for each sensor node based on its social network, and then detecting clone attacks with high probability. These protocols have high detection accuracy. Resilience can be achieved at low cost with less communication and computation overhead. This protocol suffers from high message overhead and it is not robust as well. Since nodes nearer to the base station forwards more messages from other nodes its operational lifetime is reduced.

Simple Distributed Detection (SDD) [3] attack is detected using the information available local to the nodes. Also Cooperative Distributed Detection (CDD) exploits node collaboration in order to improve the detection performance. The goal of the protocol is to detect emergent global properties. These protocols have reduced the number of false positive alarms and its revocations, with only acceptable skew error and drift error. The protocol is of high cost and suffers from reduced lifetime and requires more energy consumption. Time Domain Detection (TDD) and Space Domain Detection (SDD) [1] are proposed to tackle all the challenges from both time domain and space domain. This protocol provides high detection accuracy and excellent resilience against smart and colluding replicas. These protocols has high node detection accuracy disregarding node collision and naturally extensible to other classes of mobile networks. This protocol suffers from communication, computation and storage overhead.

Capture detection protocol [2] that leverages mobility and cooperation uses node mobility to cope with the node capture attack. It specifically relies on the meeting frequencies between honest nodes to gather information about the absence of captured nodes. The goal of this protocol is to detect the nodesas soon as they are revoked in the network. This protocol does not rely on any specific routing protocol and it is simple, efficient, and practically deployable. This protocol suffers from high communication cost and it is not applicable for scenario-inspired mobility models.

The wormhole attack [5] which is a serious threat in networks, especially against many ad hoc network routing protocols and location-based wireless security system is proposed. This protocol has efficient authentication and requires only moderate storage. It suffers from node misbehavior, and it is vulnerable to node capture attack and hence hard to isolate attacker using a software only approach.

A new randomized, efficient, and distributed (RED) protocol for the detection of node replication attacks, RED [4] is similar, in principle, to the Randomized Multicast protocol,

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

but with witnesses chosen pseudo randomly based on a network-wide seed was proposed. In RED neighbor nodes can physically check the coherence of the claimed location. But the protocol suffers from a major drawback in case if all the neighbors of a cheating node 'C' are corrupted then no node can identify 'C' as a cheater.

III. CLONE DEPLOYMENT

A node is captured, modified then cloned and introduced in large numbers in the network. These cloned nodeshave legal information, so it may participate in the network activities as the same way as honest nodes does. In replication attack capturing many nodes is hard than capturing one node and reprogramming it. The cloned nodes can launch variety of attacks; the node purposely drops some data, injects false data, initiates black hole attack, creates wormhole attack, suppresses legitimate data and monitors the communication. Therefore, an adversary may replicate captured sensors and employ them in the network to launch a variety of malicious activities. This attack is referred to as the clone attack.

IV. ASP ALGORITHM

The Area Splitting Protocol (ASP) is used to detect the clones in the WSN. It provides high detection probability when compared to other existing protocols. This protocol makes use of limited energy resources. Initially a node having high energy is selected as a base node. Depending upon the angle around thebase node, the area of the entire network is divided into equal subareas. For each subarea a node called master node is selected which sends claims collected from other nodes to the base node which in turn detects the cloned node by analyzing the claim received.

A. Topology Splitting

The ASP protocol makes use of both the centralized and clustering approach techniques. The base node makes use of the information sent by the master node from each subarea, which is a centralized approach. The clustering approach is used within each subarea. All nodes in each subarea sends claim to the master node, the master node in turn forwards the claim to the base node. The single point failure can be efficiently handled with the help of master node and the base node. Thus performance of the protocol in terms of energy and communication overhead is improved leading to increased accuracy of clone attack detection.

B. Selection of Base node

The Selection of the base node is done as shown in Figure 1 for the entire network and it is based on the maximum transmission range of that node and energy. The node capable of reaching maximum number of nodes will be having maximum transmission range. The node with high energy can be calculated using the Eqn (1):

$$E_H = E_{SEND} - E_{RECV} - E_{DISCARD(i)} \quad \textbf{(1)}$$

Where $E_H$is the node with high energy and E_{SEND} is the energy transmitted by the node and E_{RECV} is the energy received from other nodes. $E_{DISCARD(i)}$is the sum of energy consumed during transmission or reception of data. The base node is selected in order to improve the probability of node replication detection. This in turn decrease the chance of dropping location claims by malicious nodes.The energy consumption corresponding to each transmission can be formulated as Eqn [2],

$$E_T(r)=K_1 r^w + K_2 \quad \textbf{(2)}$$

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Where r is the radio transmission range, w is the path loss exponent; $K_1$is determined by the characteristic of the transmitter and the channel, and $K_2$is the transceiver energy consumption that is not related to r. Let E_r be the energy consumption of receiving, decoding, and processing data packets at the receiver.

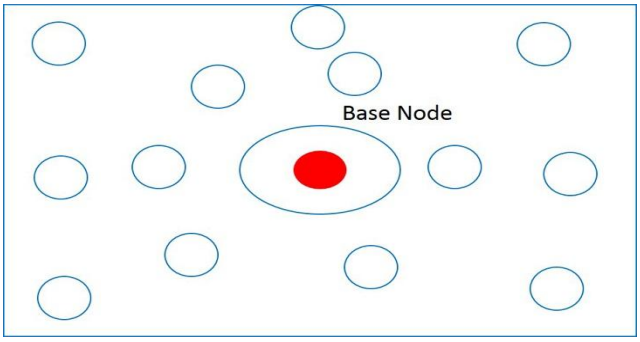

Fig.1. Base Node Selection

C. Subarea Topology Splitting

The area of the network is divided equally into a number of sub-areas as shown in Figure 2 based on the degree of angle around the base node (B) in order to assign a master node (M) for each area. The degree of angle can be around 30, 60, 90 and 120 degree and we assume to use 120 degree. The entire area should not be subdivided into very small subareas because there is a chance where the location claim sent by the master node may be lost. The formula in Eqn [3] & [4] shows the representation degree of angle.

$$E[d(\theta)] \leq S(1-p) + np \in\_(\log*(n)) \quad (3)$$

the average overall number of arcs is:

$$E[e(n)] = n[d(\theta)] \in\_(\log*(n)n) \quad (4)$$

Where S is the total area of the network, p is the loss probability, n is the number of nodes in the network.

D.Selection of Master node

A master node (M) for each subarea in the network is selected as shown in Figure 3. The node which is located in the transmission range of base node and having maximum number neighbors will be selected as a Master node. The Eqn [1] & [2] are used for selecting the base node for the whole network are applied here i.e. high energy E_H and high transmission range $E_T(r)$. The master node must also have high energy when compared with other nodes in the subarea. Each area has the angle of 120 degree around the base node. Therefore, we have three master nodes for the entire network and one base node in the network.

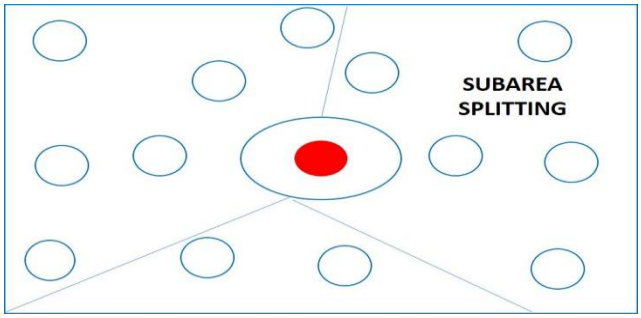

Fig.2.Subarea Topology Splitting

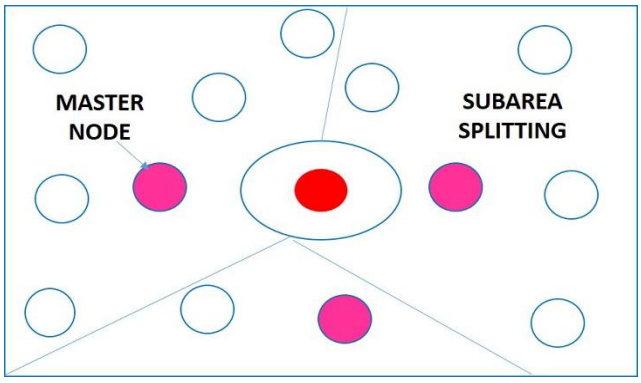

Fig.3. Master Node Selection

E. Detection of Cloned node

If the master node in any subarea receives claim from two non-coherent locations for the same identifier, then the master node will broadcast a conflicting detection message to all nodes in that particular subarea. Therefore the

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

master node could revoke the cloned identifier from the network and also makes the other nodes to avoid future transactions with the conflicting node. On the other hand if the master node in the subareas cannot detect any conflicting location claim, they will send all collected location claims to the base node. Since the base node receives all sensor nodes' location claims forwarded from the master nodes, the replication attack can be finally detected. After the base node detects location claims with the same ID but from different locations, it broadcasts the conflicting detection message to all nodes in the network. Every claim message of a node is signed with its private key which allows other nodes to identify any malicious node not abiding to the protocol.

F.Maintenance of Table

The base node maintains a table which consists of all nodes location and its identifier. When a claim is received from a master node, the base node verifies whether the ID of the node sending the claim is from same location stored in table or from a different location. If the location differs then that master node is identified as cloned node and message will be sent to all the nodes in the network to revoke that node. Hence with this table the protocol is able to detect if master nodes have been cloned.

V. ILLUSTRATION OF ASP PROTOCOL

The ASP method is illustrated in Figure 4. The node in the network say A, sends its location claim to a neighbor. Then, that neighbor node sendsthe location claim of node A, to a master node W, located near node A via intermediate nodes. Assume that an attacker A' or replica node also sends its location claim to the master node which is located near the attacker. If a master node has the location claims coming from both the original node (A) and attacker (A'), it can detect that there are conflicting location claims. Then, the master node will broadcast the conflicting detection message to all nodes in the network. On the other hand, if the master node in each area cannot detect any conflicting location claim, they will send all collected location claims to the base node. Since the base node receives all sensor nodes' location claims forwarded from the master nodes, the replication attack can be finally detected. After the base node (B) detects location claims with the same ID but from different locations, it broadcasts the conflicting detection message to all nodes.

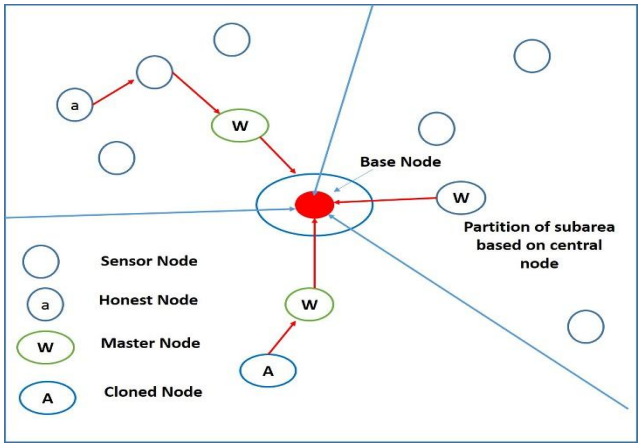

Fig.4. Illustration of ASP

Pseudo code 1: Area Splitting Protocol

Procedure to select the Base Node B ∀ S

$B \rightarrow E_H$ & $E_T(r)$

$E_H \rightarrow$ Calculate E_{SEND}, E_{RECV}, $E_{DISCARD(i)}$ ∀n(i)

$E_H \rightarrow E_{DISCARD(i)}$ is minimum

$E_T(r) \rightarrow$ Determined by K_1, K_2 not related to r

end Procedure

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Procedure S(S1, S2,S3…)

d(θ) → degree of angle around E_H

Split S into S_1, S_2, S_3

d(θ) → max

end Procedure

Procedure Select M ∀ (S1, S2,S3…)

M → E_H& $E_T(r)$

end Procedure

Procedure Claim forwarding

claim →< n(id, pos)>

To M:

nodes in S(S1, S2,S3…) fwd_claim to M

if M recv_claim for a n with same pos

M name n as cloned node(C_N)

Revoke $C_{N\&}$ broadcast a conflicting message

end M

To B:

B → receive_claim(M)

B checks if claim haves same pos

B receives claim with same pos then

follow same procedure in [To_M]

end B

end Procedure

VI. PROTOCOL EVALUATION

The attack detection can be evaluated based on the following performance metrics such as detection probability, communication overhead and network lifetime.The communication overhead represents the total number of packets forwarded during the node replication detecting process in the network. Detection probability is the percentage of successfully detecting replica node. If the number of message exchanged among the nodes gets decreased then the lifetime of the network will be increased thus leading to increased total coverage of the network.

A. Communication Overhead

Figure 5 shows that ASP has very low communication overhead when compared to Line selected multicast (LSM) method. The general requirement of ASP is that the overhead generated by the protocol should be less and should be sustainable by the WSN as a whole, and evenly shared among the nodes. Since ASP node sends their claim only to one master node in each subarea communication overhead will be very low, whereas LSM sends their claims to all node in the area. Communication overhead means the number of packets forwarded for detecting node replication.

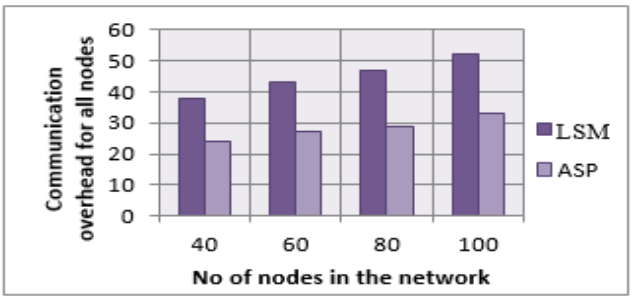

Fig.5.Comparison between ASP and LSM based upon communication overhead

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

B. Probability Rate

Figure 6 shows that ASP has high detection probability when compared to LSM protocol. ASP method makes use of both the master node as well as base node to verify the claim forwarded by other nodes in the network. Since it collects all claims it will detect the clone attack easily. In LSM, no base node is present to collect all claims so it has low detection probability. The ASP protocol has 93.7% successful detection rate.

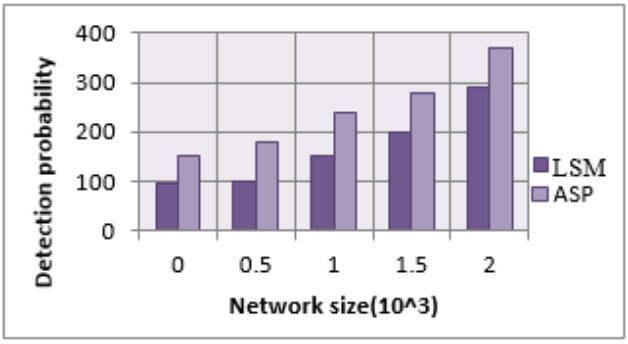

Fig.6.Comparison between ASP and LSM based upon detection probability

C. Energy Consumption

Figure 7 shows that ASP consumes less energy when compared to LSM protocol. In LSM every forwarding node is required to verify the signature of the received claim. This digital signature verification has to be done with an energy cost. ASP does not require any signature verification so very less energy is discharged. In ASP, nodes exhaust less energy whereas in LSM more energy is exhausted.Hence ASP has an increased network lifetime.

D. *Delivery Ratio*

Figure 8 shows that ASP delivers the packet in high ratio when compared to the LSM protocol. ASP makes use of master node as well as the base node to ensure that the packets are received by the nodes successfully. But LSM have no such mechanism. Figure 8 show that ASP has high delivery ratio when compared to LSM protocol.

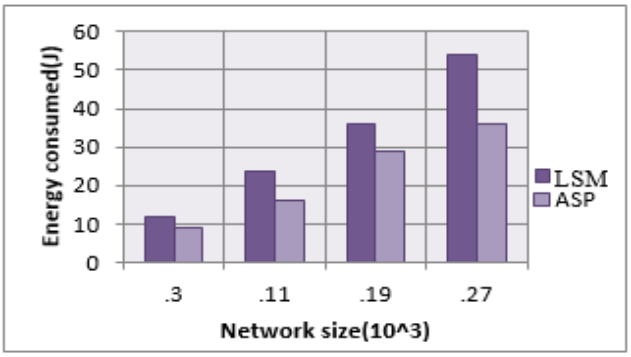

Fig.7.Comparison between ASP and LSM based upon energy consumption

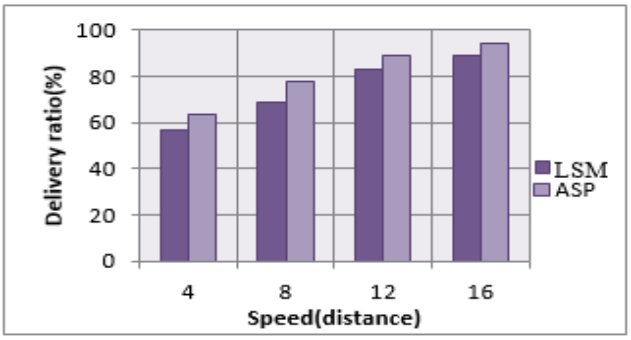

Fig.8.Comparison between ASP and LSM based upon delivery ratio

Table 1 Simulation Setup

Degree of angle	120
No of subarea	3
Node density	Fixed
Transmission range	120 m
Initial battery level	100 j
Size of data packet	512 bits
Period of simulation	1 day
Updating period	Every 60 sec

Table 1 shows the simulation setup for ASP implementation where the number of nodes, subareas, node density, size of data. Table 2 summarizes the comparisons between LSM and ASP protocols for the parameters delivery ratio

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

D_R, energy consumption E_C, delivery ratio D_P and finally communication overhead C_O.

Table 2 Simulation Setup

Parameters	LSM	ASP	No of nodes / network size / speed
D_R	74.5%	81.1%	4,8,12,16
E_C	31.5%	22.75%	.3,.11,.19,.27
D_P	75%	93.2%	0,.5,1,1.5
C_O	43%	28.2%	40,60,80,100

VII. CONCLUSION

A new clone attack detection approach called Area Splitting Protocol (ASP) method for wireless sensor networks is introduced in this paper. The proposed ASP method gives higher performance when compared with other existing protocols like Center Method, Line Selected Method, Randomized Multicast and RED protocol. The simulation results shows that the proposed ASP method can achieve high successful detecting replica rate with small amount of communication overhead. Although the ASP requires more memory capacity to store location claims in the base node, the proposed ASP method can easily support 1000 sensor nodes or more in a network. The proposed ASP method can also efficiently improve the performance of centralized approach. The proposed ASP method is simple and efficient for clone attack detection in wireless sensor networks.

REFERENCES

[1] Kai Xing, Xiuzhen Chang, "From Time Domain to Space Domain: Detecting Replica Attacks in Mobile Ad-hoc Networks in two Replication Detection Schemes",IEEE INFOCOM 2010.

[2] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, "Mobility and Cooperation to Thwart Node Capture Attacks in Manets," J. Wireless Comm. and Networking. Feb. 2009.

[3] M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei, "Emergent Properties: Detection of the Node-Capture Attack in Mobile Wireless Sensor Networks," Proc. ACM Conf. Wireless Netwok Security (WiSec '08), pp. 214-219, 2008.

[4] Mauro Conti, Robert Di Pietro Luigi V.M "Distributed detection of clone attack using RED protocol" vol.8, no.5.2011.

[5] Y.C. Hu, A. Perrig, and D.B. Johnson, Proc"Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE INFOCOM '03, pp. 1976-1986, 2003.

[6] Kai Xing, Fang Liu, ".Real-time Detection of Clone Attacks in Wireless Sensor Networks,"28th International Conference on Distributed ComputingSystem Sep. 2007.

[7] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution," IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev., vol. 37, no. 6, pp. 1246-1258, Nov. 2007.

[8] H. Choi, S. Zhu, and T.F. La Porta, "SET: Detecting Node Clones in Sensor Networks," Proc. Int'l Conf. Security and Privacy in Comm. Networks and the Workshops (SecureComm '07), pp. 341-350, 2007.

[9] M. Demirbas and Y. Song, "An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks," Proc. Int'l Symp. World of Wireless, Mobile and Multimedia Networks (WOWMOM '06), pp. 564-570, 2006.

[10] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Playing Hide-and-Seek with a Focused Mobile Adversary in Unattended Wireless Sensor Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1463-1475, 2009.

[11] Conti, Mauro, et al. "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks." Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2007.