2012 International Conference on Information and Computer Networks (ICICN 2012)
IPCSIT vol. 27 (2012) © (2012) IACSIT Press, Singapore

A Range-based Detection Method of Replication Attacks in Wireless Sensor Networks

Huang Jian[1], Xiong Yan[1+], Li Ming-xi[1], Miao Fu you[2]

(School of Computer Science and Technology, University of Science and Technology of China)

Abstract. Node replication attack is a common attack mode in wireless sensor networks. Attackers capture certain sensor nodes, replicate them and deploy several replicas back into the network for further malicious activities. A number of protocols have been proposed so far to tackle node replication attacks. However, to the best of our knowledge, none of these schemes are suitable for mobile wireless sensor networks because most of simple distributed solutions need to use node positions, system synchronous clock and other Characteristic data. In this paper, we propose a range-based detection method (RBDM) to detect replication attacks in wireless sensor networks. In this method, wireless ranging information between nodes is used to detect node replication attacks. The method can maintain a high probability of detection with Low accuracy ranging between nodes. Our theoretical analysis and simulation results show that the method is efficient and practical in detection of replication attacks in wireless sensor networks

Keywords: wireless sensor networks,detection of replication attacks, Range-based detection methods.

1. Introduction

Wireless Sensor Network (WSN) is a spatially distributed wireless network which consists of low-cost autonomous devices called "sensor nodes" that has sensors and wireless communication capabilities. WSN are often deployed in harsh environments in both military and civil applications, where staff is not easy to live [1], [2]. With the development of wireless sensor networks, building a wireless sensor networks requires not only constituting nodes, wireless communication protocols and routing protocols but also suitable Security protocols [3].Due to the unattended and not equipped with the tamper-resistance hardware, the adversary could capture some sensors, and then acquire all the information stored within [4]-[6]. There are a number of schemes been proposed for preventing and detecting node replication attacks in wireless sensor networks [7], [8]. Many simple distributed solutions for detection of node replication attacks in wireless sensor networks can be designed using multi-hop communication, and these solutions need system information claims, which include system synchronization time, precise node location information and so on: (1) Use time-location claims is a simple resolution for detection of replication attacks in WSN [9]-[11]. However, this scheme requires system synchronization time and precise node location information. The cost is so significant that many wireless sensor networks cannot afford, in view of the fact that it considerably reduces their lifetime; (2) The other resolution can protect WSN from replication attacks by data encryption [12]-[14]. A number of encryption protocols have been proposed so far to tackle node replication attacks. However, this scheme requires more computing power of the nodes, Due to the limited resources of nodes, this scheme is not suitable for detection of node replication attacks in mobile wireless sensor networks; (3) We can also protect WSN by using other characteristic data of networks [15], [16]. There are many kinds of characteristic data of networks can be use to detect replication attacks, but Additional equipments are required to be Installed on the nodes for data collection which increase the power consumption of these

[+] Corresponding author. Tel.: +86 0551-3607394; fax: +86 0551-3607394.
E-mail address: yxiong@ustc.edu.cn

nodes.In this paper, a range-based detection method (RBDM) is proposed for detecting node replication attacks in wireless sensor networks. The protocol defines three detection criterions: Local Unique ID

Criterion (LUIC), Neighbor Unique ID Criterion (NUIC) and Global Unique ID Criterion (GUIC). On LUIC and NUIC, nodes analysis its own neighbor-information table to detect replication attacks. On GUIC, we detect replication attacks by comparing neighbor-information tables of different nodes.

2. Related Work

The detection protocol proposed in this paper based on ranging between nodes. Taking into account the factor that the node is limit on power and size, many application systems of WSN are often use low-precision ranging module. In addition, the higher precision ranging the more cost should be pay for a system.There are a number of schemes can be used to estimate the distance between nodes. Most localization methods depend on three types of physical variables measured by or derived from sensor readings for localization: time of arrival, time difference of arrival, angle of arrival and received signal strength indicator (RSSI) [17]. We tackle the problem of using the RSSI as a distance estimator for Range-based detection, as it is available on most commercial platforms, such as those which implement ZigBee; consumes little energy and is highly scalable. However, accuracy problems are widely known.

The rest of this paper is organized as follows: In Section 3, we provide our assumptions and supply a summary of notation used throughout the paper; Section 4 described detail issues in ranging-assisted protocol; Section 5 is security and efficiency analysis of the protocols; after that, we show some experimental and simulation results in Section 6; finally, conclusions and future work to our research are given in Section 7.

3. Background

3.1. Assumption

We assume that sensor nodes in the network have unique identification and adversary which cannot create new IDs for nodes (Newsome et al. describe several techniques to prevent the adversary from deploying node with arbitrary IDs [18]), so the adversary must capture and replicate a legitimate node； A number of protocols have been proposed to detect the movement of nodes in wireless sensor network, so we assumed that adversary cannot move compromised nodes or remove it； We suppose a region called S_{re}, in which n sensor nodes has been random uniformly distributed. For our purpose, we neglect the impact of shape and edge； We also assume that the detection range of each node is R, meanwhile the impact of nodes' shape and size on communication is negligible； Since the main focus of this paper is on providing a solution to detect node replication attack, we assume the availability of a message freshness mechanism, to prevent replication attacks, have been adopted in our protocols.

3.2. Adversary model

In our problem settings, sensor nodes are not tamper-resistant. The adversary has the capability of capturing and compromising a limited number of legitimate nodes in the network. After compromising a legitimate node, the adversary can replicate the compromised node. Note that the replicas have all the legitimate information from the compromised node. Thus, the replicas can easily participate in the network operation without being identified. The basic operation of this protocol is as follows: every sensor node has its own unique identification. When communicating with each other, the node which received data detects the RSSI of the communication and records the other node is near or far away. If a sensor node's identification be found in different area, it announces the detection of a replica.

3.3. Notation

For clarity, Table 1 lists the symbols and notations used in this paper.

TABLE 1. Symbols and notations

n	Number of nodes in network
S_{re}	The region of network
S	The area of the region S_{re}
x, x'	The identification of a compromised node and its replica
x_i	The unique identity of a sensor node
R	The detection range of each node
$\|x_i - x_j\|$	The distance between x_i and x_j

4. The Range-based Detection Method of the Replication Attacks

In this section, we propose to design a new distributed approach which does not require any nodes graphic position messages or system time synchronization for detecting node replication attacks in wireless sensor networks. The fundamental idea is to make use of the unique identification property: If a node has been detected, it could not appear in any other area. The RBDM is a range-based distributed detection method. In this paper, we use RSSI to estimate the distance between nodes. Each node estimates the distances between it and its neighbors by RSSI and executes the following two steps:

(Step 1) Categorizing neighbors:

We suppose that node a is a neighbor of node b(that is $|x_a - x_b| \le R$). If $|x_a - x_b| \le R/2$, they are a pair of close neighbors, otherwise called far neighbors.

(Step 2) Constructing the detection information table of neighbors:

Each node records all identifications of its neighbors and set a flag signify their categorization. All of this information is stored in the neighbor-information table (as show in Fig. 1).

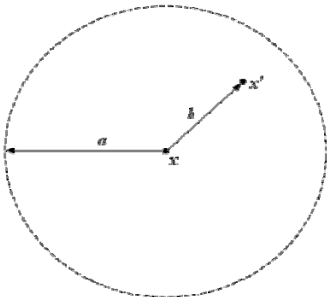
TABLE 2. Neighbor-information table

FLAG	01	00	00	...	00
ID	6	9	8	...	7

Nodes in the network periodically broadcast own neighbor information table. By comparing nodes' neighbor-information table, we can detect replication attacks.In the following, we present three comparing criterion. When any of criterion in force, it means that replication attacks has been detected.

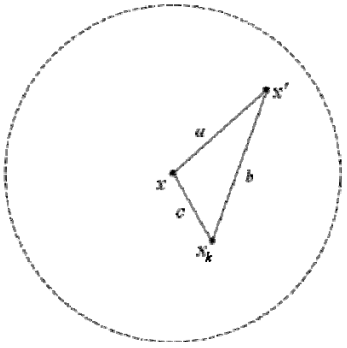
4.1. LUIC: Local Unique ID Criterion

As shown in Fig. 1, if a replica x' has been deployed in the detection range of the compromised node x, they can detect each other (it means $|x - x'| \le R$).



$a = R$, $b \le R$

Fig. 1 LUIC: Local Unique ID Criterion



$R < a < \frac{3R}{2}$, $\frac{R}{2} \le b \le R$, $c \le \frac{R}{2}$

Fig. 2 NUIC: Neighbor Unique ID Criterion

In this case, a same identification appears in the neighbor-information table of x, so that the LUIC come into force.

4.2. NUIC: Neighbor Unique ID Criterion

Generally, replica node and compromised node cannot detect each other. Then the NUIC might be effective if we can find a node x_k in network that can detect both replica x' and compromised node x, meanwhile x' and x are different neighbor of x_k as shown in Fig .2,

In the neighbor-information table of x_k, we can find x' and x with different flag. Then NUIC would divide into two symmetrical situations described as the following:

(Situation1)

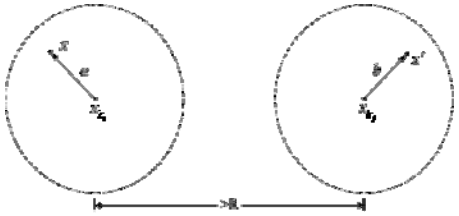
$$R < |x - x'| < \frac{3R}{2}, \frac{R}{2} \le |x - x_k| \le R \text{ and } |x' - x_k| \le \frac{R}{2};$$

(Situation2)

$$R < |x - x'| < \frac{3R}{2}, \frac{R}{2} \le |x' - x_k| \le R \text{ and } |x - x_k| \le \frac{R}{2};$$

4.3. GUIC: Global Unique ID Criterion

Obviously, the probability of LUIC or NUIC might be very low in a large region. In order to detect sparse distributed replicas, we should use neighbor-information tables of different nodes. As shown in Fig. 3, x_{k_i} and x_{k_j} find a same identification (x' or x) as a close neighbor, however they can not detect each other (it means $|x_{k_i} - x_{k_j}| > R$).



$$a \le \frac{R}{2}, \quad b \le \frac{R}{2}$$

Fig. 3 GUIC: Global Unique ID Criterion

The same as x_{k_i}, x_{k_j} can find x' (or x) is record in its neighbor-information table with flag '00' in such case. According to triangle theory, x_{k_i} and x_{k_j} might be neighbors, otherwise GUIC should be in force.The three criterions mentioned above are independent of each other, which can be test one by one in detection of replication attacks. So we can calculate the total probability of detection by weighted accumulation of criterions.There are a number of routing protocols can be used to transmit neighbor-information tables of sensor nodes. In order to achieve comparisons of neighbor-information tables without store any received information, other complex criterions by analyzing more than two nodes' neighbor-information tables will not be mentioned in this paper.

In order to see whether these criterions can be implemented as a building block of an efficient distributed methods to detect node replication attacks, we analysis detection probability in the next section.

5. Analysis

To improve the detection performance, the probabilities of three criterions are analysis in this section. Assume P_1 is the detection probability of LUIC, P_2 is the detection probability of NUIC, P_3 is the detection probability of GUIC, and we can define the total detection probability as $P = P_1 + P_2 + P_3$.

5.1. P_1: The Probability of LUIC

Because nodes ($x, x_1, x_2 \cdots x_{n-1}$) are independent uniformly distributed in the region, the probability x_i which is distributed in a position can be describe as $f(x_i)$.

$$f(x_i) = \begin{cases} \frac{1}{s}, & x_i \in S_{re} \\ 0, & x_i \notin S_{re} \end{cases} \quad (1)$$

According to the definition of LUIC (that is $|x - x'| \le R$), the probability of LUIC is

$$P_1 = \iint_{|x-x'|\le R} f(x)\cdot f(x')dS_{re} \tag{2}$$

Substituted equation (1) into equation (2), we can define P_1 as equation (3).

$$P_1 = \iint_{|x-x'|\le R} \frac{1}{s}dS_{re} = \frac{\pi R^2}{s} \tag{3}$$

5.2. P_2 : The Detection Probability of NUIC

When LUIC is not in force, NUIC might effect in the situation mention in section 4. We define situation 1 and situation 2 as following:

(Situation 1)

$$\begin{cases} |x_k - x| \le \dfrac{R}{2}, & (Condition \quad I) \\ \dfrac{R}{2} < |x_k - x'| \le R, & (Condition \quad II) \end{cases}$$

(Situation 2)

$$\begin{cases} |x_k - x'| \le \dfrac{R}{2}, & (Condition \quad I') \\ \dfrac{R}{2} < |x_k - x| \le R, & (Condition \quad II') \end{cases}$$

As given in equation (2), the probability of condition I (or condition I') can be define as

$$P(I) = \iint_{|x_k - x|\le R/2} f(x_k)\cdot f(x)dS_{re} = \frac{\pi\left(R/2\right)^2}{s} = \frac{\pi R^2}{4s} \tag{4}$$

The probability of condition II (or condition II') can be define as

$$P(II) = \iint_{R/2<|x_k - x'|\le R} f(x_k)\cdot f(x')dS_{S_{re}} = \frac{\pi R^2 - \pi\left(R/2\right)^2}{s} = \frac{3\pi R^2}{4s} \tag{5}$$

Considering that condition I and condition II are independent of each other, so the probability of situation 1 (or situation 2) is

$$P(I)\cdot P(II) = \frac{\pi R^2}{4s}\cdot\frac{3\pi R^2}{4s} = \frac{3\pi^2 R^4}{16s^2} \tag{6}$$

Similarly, we can obtain $P(I')\cdot P(II')$.

Assumed P_2' is the probability of NUIC, it can be defined as

$$P_2' = \left[P(AB) + P(A'B')\right]\cdot(1 - P_1) = \frac{3\pi^2 R^4}{8s^3}\cdot\left(s - \pi R^2\right) \tag{7}$$

In our problem settings, there are n sensor nodes have been deployed. Thus, the detection probability of NUIC is the probability that there is at least one node can satisfy both condition I (or condition I') and condition II (or condition II').

According to Bernoulli equation, we can define the detection probability of NUIC as equation (8).

$$P_2 = 1 - \left(1 - P_2'\right)^{n-1} \tag{8}$$

Substituted equation (5) into equation (6), we can obtain the expression of P_2.

5.3. P_3 : The Detection Probability of GUIC

When a sensor node receive a neighbor-information table from another node, it compare the received table to its own table for detection of replication attacks, if LUIC and NUIC have not been effected. Therefore, we should find a pair of nodes can satisfy the condition describe as follows.

(Situation 1)

$$\begin{cases} \left|x_{k_1}-x\right| \le \dfrac{R}{2}, & (Condition \quad I) \\ \left|x_{k_2}-x'\right| \le \dfrac{R}{2}, & (Condition \quad II) \\ \left|x_{k_1}-x_{k_2}\right| > R, & (Condition \quad III) \end{cases}$$

(Situation 2)

$$\begin{cases} \left|x_{k_1}-x'\right| \le \dfrac{R}{2}, & (Condition \quad I') \\ \left|x_{k_2}-x\right| \le \dfrac{R}{2}, & (Condition \quad II') \\ \left|x_{k_1}-x_{k_2}\right| > R, & (Condition \quad III') \end{cases}$$

Similar to the equation (4), the probabilities of condition I , condition II and condition III can be defined as follows.

$$P(I) = \iint\limits_{\left|x_{k_1}-x\right| \le R/2} f\left(x_{k_1}\right) \cdot f(x) dS_{re} = \frac{\pi\left(R/2\right)^2}{s} = \frac{\pi R^2}{4s} \tag{9}$$

$$P(II) = \iint\limits_{\left|x_{k_2}-x'\right| \le R/2} f\left(x_{k_2}\right) \cdot f(x') dS_{re} = \frac{\pi\left(R/2\right)^2}{s} = \frac{\pi R^2}{4s} \tag{10}$$

$$P(III) = \iint\limits_{\left|x_{k_1}-x_{k_2}\right| > R} f\left(x_{k_1}\right) \cdot f\left(x_{k_2}\right) dS_{re} = 1 - \frac{\pi R^2}{s} \tag{11}$$

Considering that condition I , II and III are independent of each other, so the probability of situation 1 (or situation 2) is

$$P(I) \cdot P(II) \cdot P(III) = \frac{\pi R^2}{4s} \cdot \frac{\pi R^2}{4s} \cdot \left(1 - \frac{\pi R^2}{s}\right) = \frac{\pi^2 R^4}{16 s^3}\left(s - \pi R^2\right) \tag{12}$$

Similarly, we can obtain $P(I') \cdot P(II') \cdot P(III')$.

Assumed P_3' is the probability of NUIC, it can be defined as equation (13).

$$\begin{aligned} P_3' &= \left[P(ABC) + P(A'B'C')\right] \cdot (1 - P_1) \cdot (1 - P_2) \\ &= \frac{\pi^2 R^4}{8 s^4}\left(s - \pi R^2\right)^2 \cdot \left(1 - P_2'\right)^{n-1} \end{aligned} \tag{13}$$

According to Bernoulli equation, P_3 can be describe as follows.

$$P_3 = 1 - \left(1 - P_3'\right)^{C_{n-1}^2} \tag{14}$$

In equation (14), the detection probability P_3 is the probability that there are at least one pair of nodes can satisfy condition I (or condition I'), condition II (or condition II') and condition III (or condition III') in the same time.

In conclusion, we can obtain the total detection probability P as the sum of P_1, P_2 and P_3.

$$\begin{aligned} P &= P_1 + P_2 + P_3 \\ &= \frac{\pi R^2}{s} + 1 - \left(1 - P_2'\right)^{n-1} + 1 - \left(1 - P_3'\right)^{C_{n-1}^2} \\ &= \frac{\pi R^2}{s} - \left(1 - P_2'\right)^{n-1} - \left(1 - P_3'\right)^{C_{n-1}^2} + 2 \end{aligned} \tag{15}$$

Where $P_2^{'} = \frac{3\pi^2 R^4}{8s^3} \cdot (s - \pi R^2)$, $P_3^{'} = \frac{\pi^2 R^4}{8s^4}(s - \pi R^2)^2 \cdot \left(1 - P_2^{'}\right)^{n-1}$.

As given in equation (15), the total detection probability P can be expressed like a function of n, s and R. Thus, we can use the function to determine suitable parameters for different applications, and then the range-based method can get a high detection probability. The simulation results in the section 6 confirm the conclusion we get in this section and improve the effectiveness of RBMR.

6. Simulations

To verify the feasibility of our method, we ran simulations to measure the detection performance of three criterions. We simulate the method inNS2.27 with IEEE 802.15.4 protocols. In the following simulations, we will consider networks with different parameters to observe the impact of different parameters on the detection probability.Firstly, we consider a network to be deployed in a region of area $s = 10000$. As shown in Fig.4, the detection probability arise with the increase in parameter n or R.

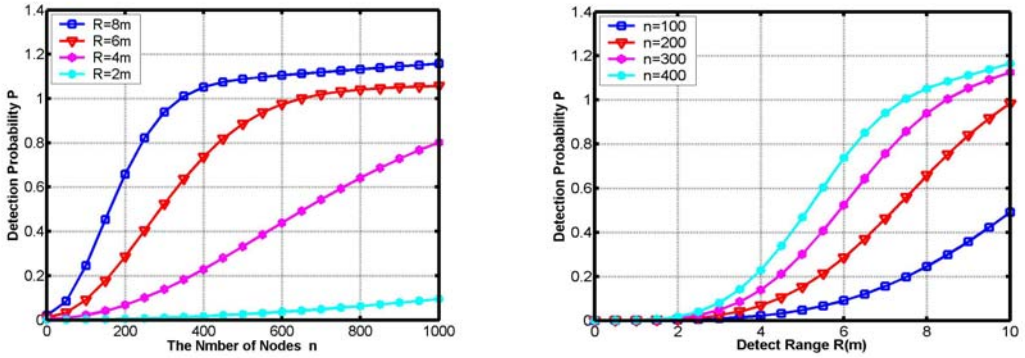


Fig. 4 Detection probability. In certain region ($s = 10000$)

In Fig.4, when parameter n and parameter R increase to a certain value, the detection probability would be close to 100%. Because three criterions are independent of each other, the detection probability might be larger than 1. When the detection probability is larger than 1, it means that a criterion has taken effect earlier.

Secondly, we set parameter $R = 3$ and the simulation result is shown in Fig. 5.

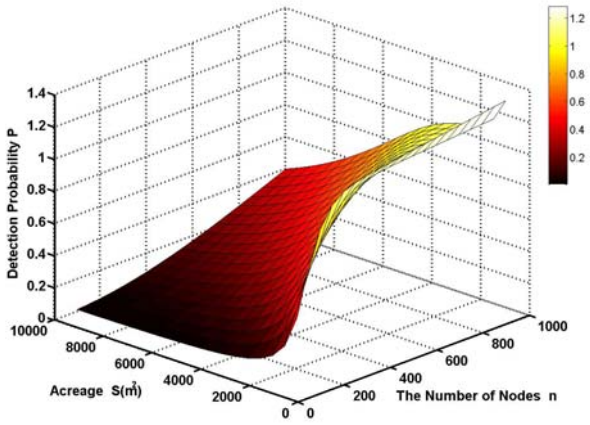


Fig. 5 Detection probability. ($R = 3$)

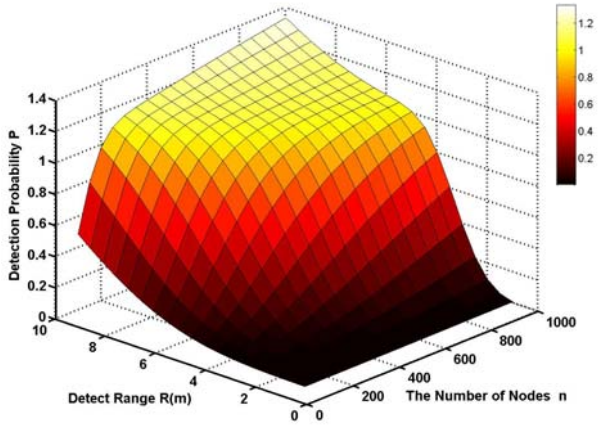


Fig. 6 Detection probability.($s = 12000$)

According to the simulation result in Fig. 5, the detection probability is low when nodes are deployed in a large area. In this case, we should increase nodes' detect range by using new nodes or installing new sensor. Next we set $s = 12000$, the simulation result in Fig.6 show the change of the detection probability with different setting of other parameters.

The simulation result shows that the number of nodes in the network can significantly affect the detection probability. When a network is consisting of a large number of sensor nodes, the detection

probability will be higher and stable. In other word, the RBDM is more suitable for the network comprising of a large number of nodes just like the WSN [19].

7. Conclusion

It is well known that the wireless ranging is a basic function of nodes [20] in wireless sensor networks. Thus, a range-based detection method (RBDM) has been supposed to detect replication attacks in this paper. The RBDM can detect replicas by all kinds of ranging method (like RSSI), so we can apply it to WSNs with different elements. The RBDM can be used like not only an independent protocol but also a sub-protocol of any other communication protocol. Our theoretical analysis and simulation results demonstrated that the RBDM have excellent detection performance, and low communication/storage overhead, without system synchronization time, precise node localization or other additional information.

8. References

[1] Xiangqian, C., Makki, K., Kang, Y., and Pissinou, N. 2009. SensorNetwork Security: a Survey, Communications Surveys Tutorials,IEEE , vol.11, no.2, pp.52-73.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. Int'l J. Computer and Telecomm.Networking, vol. 38, no. 4, pp. 393-422, 2002.

[3] Haowen, C., and Perrig, A. 2003. Security and Privacy in SensorNetworks. Computer. vol.36, no.10, pp. 103-105.

[4] Brooks R., Govindaraju P.Y., Pirretti M., Vijaykrishnan N.,andKandemir M.T. 2007. On the Detection of Clones in SensorNetworks Using Random Key Predistribution, Systems, Man, andCybernetics, Part C: Applications and Reviews, IEEE Transactionson, vol.37, no.6, pp.1246-1258.

[5] Parno, B., Perrig, A., and Gligor, V. Distributed detection of nodereplication attacks in sensor networks, Security and Privacy. 2005IEEE Symposium on , vol., no., pp. 49-63.

[6] Conti, M., Di Pietro, R., Mancini, L. V., and Mei, A. 2007. Arandomized, efficient, and distributed protocol for the detection ofnode replication attacks in wireless sensor networks. In Proceedingsof the 8th ACM international Symposium on Mobile Ad Hoc Networkingand Computing (Montreal, Quebec, Canada, September09 - 14, 2007). MobiHoc '07. ACM, New York, NY, pp. 80-89.

[7] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and AlessandroMei. Requirements and Open Issues in Distributed Detection ofNode Identity Replicas in WSN. In Proceedings of the 2006 IEEEInternational Conference on Systems, Man, and Cybernetics, pp.1468-1473. October 8-11, 2006, Taipei, Taiwan.

[8] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, andAlessandro Mei. Distributed Detection of Clone Attacks inWirelessSensor Networks. IEEE Transactions on Dependable and securecomputing, vol.8, no.5, pp. 685-698.September/October 2011.

[9] Xiaoming Deng, Yan Xiong, and Depin Chen. Mobility-assistedDetection of the Replication Attacks in MobileWireless Sensor Networks. In Proceedings of the 6th International Conference on Wireless and Mobile Computing, pp. 225-232, 2010.

[10] Jadliwala M., Sheng Zhong, Upadhyaya S.J., Chunming Qiao,Hubaux J.-P. Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes. IEEE Transactions on Mobile Computing, vol.9, no.6, pp.810-823, June 2010.

[11] Yingpei Zeng, Jiannong Cao, Jue Hong, Shigeng Zhang, Li Xie.SecMCL: A Secure Monte Carlo Localization algorithm for mobile sensor networks. In Proceedings of the 6th International Conference on Mobile Ad-hoc and Sensor Systems (MASS '09), pp.1054-1059,12-15 Oct. 2009.

[12] Perrig A,Szewczyk R, et al. SPINS: Security protocol for sensornetworks. Wireless Networks, 2002, 8(5): 521-534.

[13] Sarmad Ullah Khan, Luciano Lavagno, and Claudio Pastrone. A Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Networks. In Proceedings of the 6th International Conference on Emerging Technologies (ICET), pp. 364-369, 2010.

[14] Chakib Bekara, Maryline Laurent-Maknavicius. A New Protocol for Securing Wireless Sensor Networks Against Nodes ReplicationAttacks. In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), pp.59-59, 2007.

[15] Heesook Choi, Sencun Zhu, Thomas F. La Porta. SET: Detecting node clones in Sensor Networks. In Proceedings of the 3rd International Conference on Security and Privacy in CommunicationsNetworks and the Workshops (SecureComm 2007), pp. 341-350,2007.

[16] Wen Tao Zhu. Node Replication Attacks inWireless Sensor Networks:Bypassing the Neighbor-Based Detection Scheme. In Proceedings of the International Conference on Network Computing and Information Security, pp . 156-160, 2011.

[17] Eugen COCA, Valentin POPA, and Georgiana BUTA. Wireless Sensor Network Nodes Performance Measurements and RSSIEvaluation. In Proceedings of the 15th International Symposium for Design and Technology of Electronics Packages, Gyula, Hungary,September 2009. 2009. 105-112.

[18] Newsome, J., Shi, E., Song, D., Perrig, A. , The Sybil attack in sensor networks: analysis defenses, Information Processing in SensorNetworks, 2004. IPSN 2004. Third International Symposium on , vol., no., pp. 259- 268, 26-27 April 2004.

[19] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. Wireless sensor networks: a survey. Computer Networks, vol.38, no.4,pp.393-422, 2002.

[20] K. Whitehouse, C. Karlof, D. Culler. A practical evaluation of radio signal strength for ranging-based localization. ACM SIGMOBILE MC2R, vol.11, no.1, pp.41-52, 2007.