A Range-assisted Detection Protocol against Replication Attacks in WSNs

Mingxi Li, Yan Xiong, Wenchao Huang and Xiancun Zhou, Xuangou Wu
School of Computer Science and Technology
University of Science and Technology of China, USTC
Hefei, China, 232007
keeperlmx@gmail.com, yxiong@ustc.edu.cn, huangwc@ustc.edu.cn, zhouxcun@mail.ustc.edu.cn, wxgou@ustc.edu.cn

***Abstract*—Wireless sensor networks (WSNs) consist of a large number of sensor nodes which are deployed without self-defense capability. The node replication attack is a specific attack mode to WSN and the detection of node replication attacks in WSNs became a fundamental problem. In this paper, we proposed a range-assisted distributed protocol (RADP) to detect node replication attacks in WSNs. The contributions of this work are threefold. First, we showed that the known solutions do not completely meet our requirements. Second, we tried to use wireless ranging information to detect node replication attacks. Third, we proposed a novel protocol for the detection of node replication attacks and Extensive theoretical analysis and experiment verified that it can maintain a high detection probability with low accuracy ranging among nodes.**

Keywords-wireless sensor networks; replication attacks; detection protocol; range-assisted.

I. INTRODUCTION

A Wireless Sensor Network (WSN) can be deployed in harsh environments to satisfy both military and civil applications, where staff is not easy to stay [1], [2]. With the development of wireless sensor networks, building a wireless sensor networks requires suitable security protocols [3]. Replication attack (or clone attack) is a common attack mode in WSNs [4]-[5]. Replicas can launch a variety of attacks such as creating a black hole or initiating a wormhole attack [6]-[8]. There are a number of solutions for detecting node replication attacks in wireless sensor networks [9], [10].

By analyzing different characteristic data of networks, distributed solutions can be simply divided into three types:

(1) Using time-location claims is a simple resolution for detection of replication attacks in WSNs [11];

(2) The other resolution can protect WSN from replication attacks by data encryption [12];

(3) We can also protect a wireless sensor network by using other characteristic data of networks [13].

In this paper, a range-assisted detection protocol (RADP) is proposed for detecting node replication attacks in wireless sensor networks without other system information but the distances between nodes.

The rest of this paper is organized as follows: Some important technologies and thesis of WSNs has been introduced in Section II; Section III described the protocol in detail; Section IV is the analysis of the protocol; we show some experiment results in Section V; finally, conclusions and future work to our research are given in Section VI.

II. RELATED WORK

A. Assumptions

We assumed that sensor nodes in the network have unique identification which cannot be created (Newsome et al. describe several techniques to prevent the adversary from deploying node with arbitrary IDs [14]).

Since the main focus of this paper is to provide a solution to detect node replication attack, we assumed that a message fresh mechanism is available, which has been adopted in our protocols to prevent replication attacks in WSNs.

B. Adversary model

Adversaries have the capability of capturing and compromise a limited number of legitimate nodes in our problem settings. Thus, the replicas can easily participate in the network operation without being identified.

C. Notation

To clarity, Table 1 lists the symbols and notations.

TABLE I. SYMBOLS AND NOTATIONS

n	Number of nodes in network
s	The area of the region
x , x'	A compromised node and its replica
x_i	The unique identity of node i
R	The transmission range of each node
R_c	The maximum distance between node and its close neighbors
R_f	The minimum distance between node and its far neighbors
α	The maximum deviation of RSSI (by training)

III. THE RADP

(Definition 1) Categorizing neighbours:

We supposed that node a is a neighbour of node b (that is $|x_a - x_b| \le R$). If $|x_a - x_b| \le R_c$, they are a pair of close neighbours, and if $R_f \le |x_a - x_b| \le R$, they are called a pair of far neighbours.

(Definition 2) Calculating R_c and R_f :

We express α as the maximum ranging deviation. To consider the impact of *RSSI* deviation, we can definite $R_c = R/2 - \alpha$ and $R_f = R/2 + \alpha$ then $\alpha < R/2$.

(Definition 3) Constructing the detection information table of neighbours:

All of its neighbours' information is stored in the neighbour-information table (as show in Table 2).

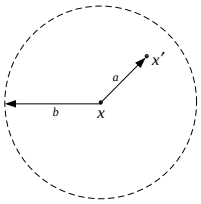
TABLE II. NEIGHBOUR-INFORMATION TABLE

Flag	01	00	00	…	00
Node ID	06	09	08	…	13

By comparing nodes' neighbour-information tables, we can detect replication attacks.

A. *LUC: Local Unique Criterion*

As shown in Fig.1, when the replica x' and node x can detect each other ($|x - x'| \le R$), LUC come into force.

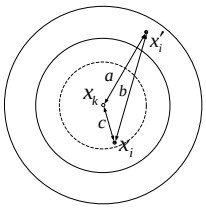


$a = R$, $b \le R$

Figure 1. LUC: Local Unique Criterion

B. *NUC: Neighbour Unique Criterion*

We can find a node x_k when both replica x' and compromised node x be detected, meanwhile x' and x are different kind neighbours of x_k as shown in Fig .2.



$R < a < R + R_f$, $R_f \le b \le R$, $c \le R_c$

Figure 2. NUC: Neighbour Unique Criterion

Then NUC would be divided into two symmetrical situations described as the following:

(Situation1)

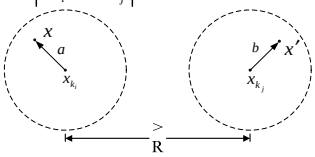
$R < |x - x'| < R + R_f$, $R_f \le |x - x_k| \le R$ and $|x' - x_k| \le R_c$;

(Situation2)

$R < |x - x'| < R + R_f$, $R_f \le |x' - x_k| \le R$ and $|x - x_k| \le R_c$;

C. *GUC: Global Unique Criterion*

As shown in Fig.3, when x_{k_i} and x_{k_j} find a same identification (x' or x) as a close neighbour but they cannot detect each other ($|x_{k_i} - x_{k_j}| > R$), GUC come into force..



$a \le R_c$, $b \le R_c$

Figure 3. GUC: Global Unique Criterion

IV. ANALYSIS

A. P_1: *The Probability of LUC*

Because nodes are independent uniformly distributed, the distributed probability of x_i can be describe as:

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

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

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

Substituted (1) into (2), we can define P_1:

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

B. P_2: *The Detection Probability of NUC*

(Situation 1)

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

(Situation 2)

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

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

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

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

$$P(II)=\iint_{R_f<|x_k-x'|\le R} f(x_k)\cdot f(x')\,dS_{S_{re}}=\frac{\pi R^2-\pi\left(\frac{R}{2}+\alpha\right)^2}{s} \quad (5)$$

The probability of situation 1 (or situation 2) is

$$P(I)\cdot P(II)=\frac{\pi^2(R-2\alpha)^3(3R+2\alpha)}{16s^2} \quad (6)$$

Similarly, we can obtain $P(I')\cdot P(II')$. Assumed P_2' is the probability of NUC, it can be defined as

$$\begin{aligned}P_2'&=\left[P(I)P(II)+P(I')P(II')\right]\cdot(1-P_1)\\&=\frac{\pi^2(R-2\alpha)^3(3R+2\alpha)}{8s^3}\cdot\left(s-\pi R^2\right)\end{aligned} \quad (7)$$

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

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

C. P_3 : The Detection Probability of GUC

(Situation 1)

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

(Situation 2)

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

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

$$P(I)=\iint_{|x_{k_1}-x|\le R_c} f(x_{k_1})\cdot f(x)\,dS_{re}=\frac{\pi(R-2\alpha)^2}{4s} \quad (9)$$

$$P(II)=\iint_{|x_{k_2}-x'|\le R_c} f(x_{k_2})\cdot f(x')\,dS_{re}=\frac{\pi(R-2\alpha)^2}{4s} \quad (10)$$

$$P(III)=\iint_{|x_{k_1}-x_{k_2}|>R} f(x_{k_1})\cdot f(x_{k_2})\,dS_{re}=1-\frac{\pi R^2}{s} \quad (11)$$

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

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

Similarly, we can obtain $P(I')\cdot P(II')\cdot P(III')$. P_3' is the probability of NUC, it can be defined as

$$\begin{aligned}P_3'&=\left[P(I)P(II)P(III)+P(I')P(II')P(III')\right]\cdot(1-P_1)\cdot(1-P_2)\\&=\frac{\pi^2(R-2\alpha)^4}{8s^4}\left(s-\pi R^2\right)^2\cdot\left(1-P_2'\right)^{n-1}\end{aligned} \quad (13)$$

According to Bernoulli equation, P_3 can be describe as

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

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

$$P=\frac{\pi R^2}{s}-\left(1-P_2'\right)^{n-1}-\left(1-P_3'\right)^{C_{n-1}^2}+2 \quad (15)$$

V. EVALUATION

A. Simulation Evaluation

To verify the feasibility of the RADP, we ran it in NS2 with $s=10000$, $n=200$, $1\le R\le 10$ and α ={0.1×Distance ,0.2×Distance, 0.3×Distance } as shown in Fig.4.

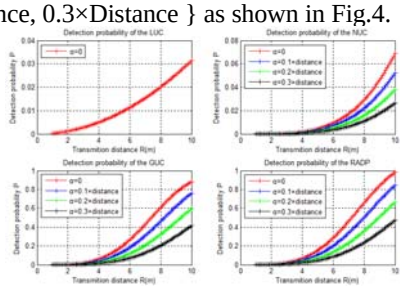


Figure 4. Detection probability of certain criterion with different α

The simulation results verified that the RADP is more efficient than the RBDM [15] as shown in Fig.5.

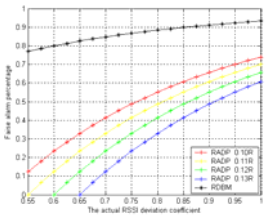


Figure 5. The percentage of false alarm in RADP and RBDM

B. Real System Evaluation

We run the RADP in a WSN experiment system called GAINS3 as shown in Fig.6.

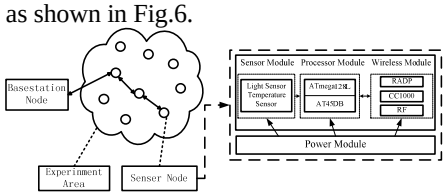


Figure 6. GAINS3 experiment system of WSN

We set an experiment area ($s = 10m \times 8m$) and deploy 30 nodes in it as shown in Fig.7.

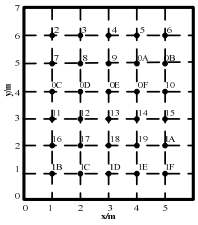


Figure 7. Real system experiment setting

The detection range of nodes is 5m and the deviation is 0.5m. All nodes run the RADP as Algorithm 1.

Algorithm 1 The RADP run in a node

1: **if** receive enough Guide frequency bytes **then**
2: get RSSI value
3: **end if**
4: Save the id (x_j) who send the frame with its RSSI value
5: **if** $|x_i - x_j| \le R_c$ **then**
6: record $flag_{x_j} = 0$
7: **else if** $R_f \le |x_a - x_b| \le R$ **then**
8: record $flag_{x_j} = 1$
9: **end if**
5: **search** the neighbor-information table of x_i
6: **if** $x_i = x_j$ **then**
7: alarm (a replica has been found)
8: **else if** exist $flag_{x_j} = 1$ and another $flag_{x_j} = 0$ **then**
9: alarm (a replica has been found)
10: **end if**
11: **search** the neighbor-information table of x_j
12: **if** exist x_k whose $flag_{x_k} = 0$ in both neighbor-information tables of x_j and x_i , but x_i and x_j is not a pair of neighbors **then**
13: alarm (a replica has been found)
14: **end if**
15: **end search**
16: **end search**

Our real system experiment result confirmed that the RADP is more suitable for the network comprising of a large number of nodes just like the WSN.

VI. CONCLUSION

The RADP can be used as not only an independent protocol but also a sub-protocol of any other communication protocol. Our theoretical analysis and simulation results demonstrated that the RADP achieves excellent detection performance, low communication and false alarm percentage, without system synchronization time, precise node localization and other additional information.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under grant No.61170233, No.61232018, No.61272472, No.61202404, No.61272317 and China Postdoctoral Science Foundation No.2011M501060.

REFERENCES

[1] 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.

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

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

[4] S. Zhu, S. Setia, and S. Jajodia. LEAP: efficient security mechanisms for large-scale distributed sensor networks. In CCS '03, pages 62–72, 2003.

[5] Conti, M., Di Pietro, R., Mancini, L. V., and Mei, A. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. MobiHoc '07. ACM, New York, NY, pp. 80-89, 2007.

[6] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In INFOCOM '05, pages 1917–1928, 2005.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM '03, pages 1976–1986, 2003.

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

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

[10] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In Security and Privacy, 2005 IEEE Symposium on, pages 49–63. Ieee, 2005.

[11] 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.

[12] Sarmad Ullah Khan, Luciano Lavagno, and Claudio Pastrone. A Key Management Scheme Supporting Node Mobility in Heterogeneous Sensor Networks. In ICET 2010, pp. 364-369, 2010.

[13] 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 SecureComm 2007, pp. 341-350,2007.

[14] Newsome, J., Shi, E., Song, D., Perrig, A. , The Sybil attack in sensor networks: analysis defenses. The Information Processing in SensorNetworks (IPSN2004), pp. 259- 268, 26-27 April 2004.

[15] HUANG Jian, XIONG Yan, LI Mingxi, MIAO Fuyou. A Range-based Detection Method of Replication Attacks in Wireless Sensor Networks. In ICICN 2012, vol. 27, pp. 120-127, 26-28 February 2012.