

# Study on Automatic Positioning of Malicious Mobile Nodes in Wireless Sensor Networks

Zheng Wen-kui\*<sup>1a</sup>, Liu kun<sup>1b</sup>

<sup>1</sup>: School of Software, Henan University, Kaifeng 475004, China

zhengwenkuisja@163.com

**Keywords:** Wireless sensor networks; Malicious; Mobile node; Automatic positioning

**Abstract.** The automatic positioning method of malicious mobile nodes in wireless sensor networks is one of the security content of wireless sensor networks, which has the extremely important research significance. In the traditional wireless sensor networks, the location of the malicious mobile nodes needs to be provided support by the regional monitoring of the nodes under attack. The power consumption and cost are greatly limited. Therefore, we proposed a fuzzification malicious mobile node positioning algorithm, which was based on the existing network node positioning function and the MONTE CARLO positioning algorithm. It filtered the periodical information for fuzzy processing, which could still be highly accurate positioning under the asking with smaller communication data. The simulation results show that the proposed method is simple, the interface and port are uniform, and the computing speed and positioning accuracy are improved.

## Introduction

With the development of science technology and network technology, the wireless communication technology and technology in sensor field has achieved rapid development. Wireless sensor technology has changed from single to integrated, networked and intelligent. Wireless sensor network has the wireless communication capabilities, involving with many domains.

In the traditional wireless sensor network, the method of obtaining malicious mobile node positioning needs the support of the infrastructure. So the consumption is high, and the system scalability is poor, and the positioning cost is high, which seriously influences and restricts the development space of wireless sensor networks.

Therefore, we proposed a fuzzification malicious mobile node positioning algorithm, which was based on the existing network node positioning function and the MONTE CARLO positioning algorithm. It filtered the periodical information for fuzzy processing, which could still be highly accurate positioning under the asking with smaller communication data. The simulation results show that the proposed method is simple, the interface and port are uniform, and the computing speed and positioning accuracy are improved.

## An overview of malicious mobile node positioning in Wireless Sensor Networks

### A. Wireless sensor network architecture

In wireless sensor networks, the data of each node is huge. These nodes are usually randomly arranged by the manual mode. Wireless connection among all nodes forms a wireless sensor network. These nodes interact with each other and process the data, and finally All information nodes are clustered by the way of multi-hop routing. The detailed construction diagram is shown in figure 1.

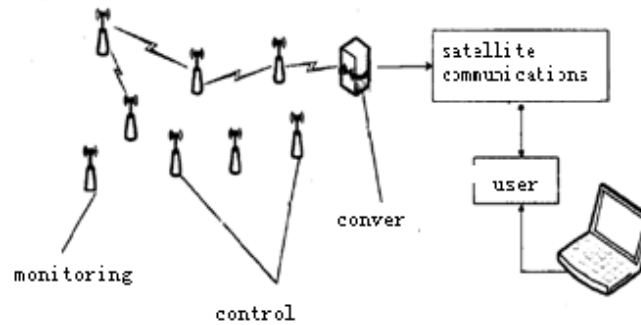


Figure 1. Structure chart of wireless sensor network

Generally, the composition mode and structure of nodes in wireless sensor networks are different. But, all wireless sensor networks include Power supply, data acquisition module, data transmission system and the data processing module. The data acquisition part is composed of the wireless sensor and analog digital conversion system, which mainly realizes the data transmission and data conversion.

**B. Structure of wireless sensor node**

The wireless sensor networks are usually deployed in relatively practical application environment. According to the actual environment, the size and power consumption of the hardware equipment are needed to be considered. In general, from the hardware, the actual wireless sensor nodes are mainly divided into five parts:

The controller module is mainly to run the code in wireless sensor networks and control the data information of the nodes in the sensor network.

The memory module is mainly to run the protocols and algorithms, which is generally composed of RAM and ROM.

Sensing equipment module is the interface of the peripheral sensor equipment, such as the temperature sensor. It is mainly used to measure the environmental parameters.

Wireless devices is mainly responsible for receiving data and information. The more commonly used is the 802.15.4 communication technology, and the blue tooth and 802.11B technology are frequently used.

The energy equipment is mainly responsible for providing energy to each node in the wireless sensor network, which is likely to be battery powered. It also uses solar energy and other environmental energy in specific conditions. As shown in figure 2.

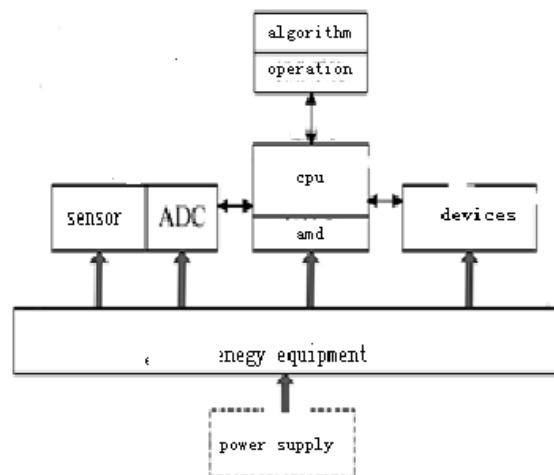


Figure 2. Architecture diagram of sensor node

**Automatic positioning of malicious mobile nodes**

In wireless sensor networks, the sensors generally use the cheap sensor node. Therefore, it is easy to be attacked malicious mobile node attacks. The malicious node positioning is the emphases

and difficulty in the research of wireless sensor network. At this stage, the main methods are the ranging algorithm and the unrelated ranging algorithm.

**A. Overview of fuzzy positioning algorithm**

The process of fuzzification positioning is the process of the intercommunication of the results of malicious mobile nodes which accord with the collected information. In the process of positioning, it is the corresponding relationship between the information of the hitting and scolding information received and the actual position of the malicious node information. The temperature and humidity factors of the transmission are considered in practical applications. But, there are many objective influences of malicious mobile nodes, and the results are unstable.

Fuzzification positional method is to change the original node information for the fuzzification information, which reduces a lot of interference factors, Then, the fuzzification node information is matched with the malicious mobile node information. The parameters are modified to obtain the relatively stable malicious mobile node positioning in wireless sensor networks.

**B. Fuzzification process**

Set the whole wireless sensor network is  $U$ , then all of the wireless sensor node set on  $U$  is used  $A$  to represent.  $\mu(u)$  is defined as:

$$\mu A : \begin{cases} U \rightarrow [0,1] \\ \mu \rightarrow \mu A(u) \end{cases} \quad (1)$$

The function  $\mu A$  is degree of membership of wireless sensor networks. For the whole wireless sensor network,  $\mu A(u)$  reflects the degree of membership of nodes to the fuzzification set  $A$  in the whole network. When the value is closer to 1, the higher the degree of the nodes belonging to  $A$  in the sensor network.

The relationship of administrative subordination of wireless sensor network malicious node can be constructed freely under match condition. Because of the wireless sensor network malicious mobile node structure is simple. At the same time, in the whole network, the tendency can satisfy RSSI positioning characteristics in general. So it can be represented by  $rank_k$  function.

$$\mu rank_k = \begin{cases} 0, x \leq a_k - a_{k2} \\ \frac{1}{2} + \frac{1}{2} \sin \frac{\pi}{a_k - a_{k2}} [x - \frac{2a_k - a_{k2} - a_{k1}}{2}], a_k - a_{k2} < x < a_k - a_{k1} \\ 1, a_k - a_{k2} \leq x \leq a_k - a_{k1} \end{cases} \quad (2)$$

The  $m$  value of the fuzzification process reflects the fuzzification particle size of malicious mobile nodes in wireless sensor networks. When the value is increasing, the coverage of malicious mobile nodes in wireless sensor networks can be guaranteed. Then the close degree of fuzzification set  $rank_k$  will be reduced.

From the formula (2), the fuzzification method can contain malicious mobile node localization method in wireless sensor networks. The ranging procedure collects and blurs  $rank_k$ . When the sum  $m=1$ , it can be considered non-malicious nodes, when  $m \rightarrow Num(RSSI)$ ,  $m \rightarrow Num(RSSI)$  is the set of malicious mobile nodes that can be accepted. The results are sent, compared with the original RSSI information. The location of the mobile node is determined.

**Simulation Experiment**

In order to test the effectiveness of the automatic positioning method of malicious mobile nodes in wireless sensor networks, based on RSSI fuzzification detection algorithm was carried out under MATLAB. Four kinds of network malicious mobile node behavior were used for the corresponding network attacks. The building of wireless sensor network experiment platform is

shown in Table 1.

Table 1 Experimental data sheet

Experimental software or equipment	Quantity	Parameter
PC equipment	1	Intel (R) Pentium Dual
Operating system	1	3.07GHz 64GB memory Microsoft Windows 7
Simulation software	1	Matlab7.0
Experimental data source	1	KDDCUP99
Data development platform	1	Visual Studio 2012, Netframework4.5

In the wireless sensor network of the simulation experiment, the malicious mobile node will bring the attack data which attacksthe data transmission of the whole wireless sensor network. We did the comparison of detection rate between the malicious mobile node positioning detection method in traditional wireless sensor network and the proposed fuzzification nodes automatic positioning detection. As shown in Figure 3:

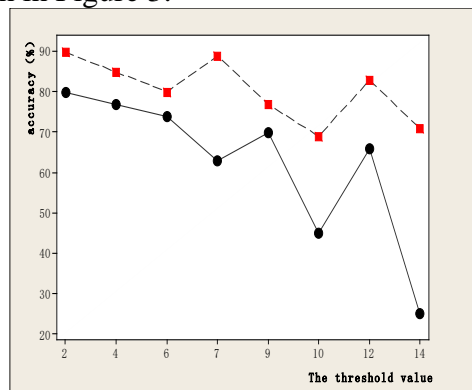


Figure 3. Comparison plot of positioning accuracy rate

For malicious mobile node automatic positioning in wireless sensor networks, the accuracy rate based on fuzzification mobile nodes automatic positioning algorithm is higher. The malicious mobile node positioning accuracy rate is significantly higher than the traditional algorithm. The adaptive ability is stronger.

In a given situation of sensor network malicious mobile node (4 kinds of known malicious mobile network nodes), the fault tolerance comparison in time and ability of process data of the traditional method and the new method is shown in figure 4:

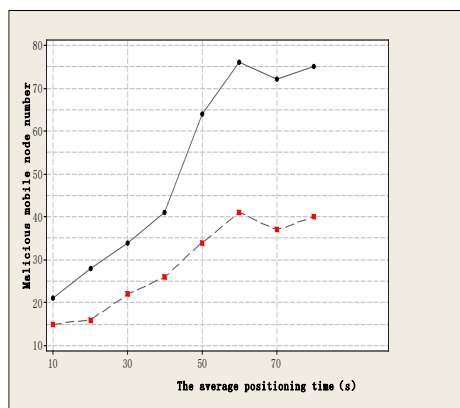


Figure 4. Comparison chart of malicious mobile node positioning time

As shown in Figure 4, in the wireless sensor network, the automatic positioning algorithm based on fuzzification malicious mobile node is faster and very accurate. The timeliness of positioning is stronger.

From the above experimental data, we can find that the automatic positioning method based on the malicious mobile node in fuzzification wireless sensor network is more accurate. The data processing ability and adaptive ability are stronger.

## Conclusion

In the traditional wireless sensor network, the method of obtaining malicious mobile node positioning needs the support of the infrastructure. So the consumption is high, and the system scalability is poor, and the positioning cost is high, which seriously influences and restricts the development of wireless sensor networks. Therefore, we proposed a fuzzification malicious mobile node positioning algorithm, which was based on the existing network node positioning function and the MONTE CARLO positioning algorithm. It filtered the periodical information for fuzzy processing, which could still be highly accurate positioning under the asking with smaller communication data. The simulation results show that the proposed method is simple, the interface and port are uniform, and the computing speed and positioning accuracy are improved.

## References

- [1] C. S. Raghavendra, Krishna M. Sivalingam, Taieb F. Znati. *Wireless sensor networks* [M]. Springer Press. 2004
- [2] Srivastava, M., Muntz, R., and Potkonjak, M. Smart kindergarten: sensor-based wireless networks for smart developmental problem-solving environments[C]. In *Proceedings of the 7th Annual international Conference on Mobile Computing and Networking (Rome, Italy)*. Mobi Com '01. ACM, New York, NY, 132-138, 2001.
- [3] Akyildiz, I.F.; Weilian Su; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks [C], *Communications Magazine, IEEE*, vol.40, no.8, pp. 102-114. Aug 2002.
- [4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *Wireless sensor networks: a survey* [C], *Computer Networks: The International Journal of Computer and Telecommunications Networking*, v.38 n.4, p.393-422, 15 March 2002.
- [5] N. Xu. *A Survey of Sensor Network Applications* [R]. Survey Paper for CS694a, Computer Science Department, University of Southern California. 2005.
- [6] Hightower, J.; Borriello, G., *Location systems for ubiquitous computing* [J], *Computer*, vol.34, no.8, pp.57-66, Aug 2001. [12] Jerrey Hightower, Gaetano Borriello. *A Survey and Taxonomy of Location Systems for Ubiquitous Computing* [R]. Technical Report UW-CSE 01-08-03. August 24, 2001
- [7] N. Priyantha, H. Balakrishnan, E. Demaine, and S. Teller. *Anchor-free distributed localization in sensor networks* [R]. Technical Report TR-892, MIT LCS, Apr. 2003.
- [8] Priyantha, N. B., Chakraborty, A., and Balakrishnan, H. *The Cricket location-support system* [C]. In *Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (Boston, Massachusetts, United States, August 06 - 11, 2000)*. Mobi Com '00. ACM, New York, NY, 32-43. .2000

## Author introduction

**Correspondence Author:** Zheng Wenkui (1982-), male (Han), Henan, Zhengzhou, master's degree, lecturer, the main research areas for algorithm analysis and network security;  
Liu Kun (1997-) male (Han), Henan Luoyang, the main research direction: Software Engineering.