



## Intrusion Detection and Proposing Security Strategies in Wireless Sensor Network (WSN)

Davoud Yazdanpanah

Master of Computer Software, Sepidan Branch, Islamic Azad University, Sepidan, Iran

### ABSTRACT

Today, wireless sensor networks (WSNs) are considered as an ideal solution for surveillance and controlling application such as traffic control, environment surveillance, battlefield surveillance, etc. In WSNs, thousands of sensor nodes expanded in a wide and control free environment are used. These networks are mostly influenced by various attacks including Sybil attacks. In Sybil attacks, a destructive node creates several fake identities for itself. Deceiving network nodes, this node disturbs operations such as voting, data integration, fair resources allocation, and anomaly detection. This fact, in its own, is a serious threat for WSNs. In this case study, after investigating the available attacks to detect Sybil attacks in WSNs, we employed a method distributed with mobile agents and temporal information to detect Sybil attacks. Packets loss rate was also evaluated before and after using the proposed strategy.

**Keywords** Wireless Sensor Networks; Security; Secure Routing; Sybil Attacks; Attack Coping Strategies.

### INTRODUCTION

A WSN consists of a great number of sensor nodes scattered in the environment and used to measure some physical quantities or environmental conditions. WSNs were developed with the aim of surveillance battlefields. However, today, they are used for many

non military purposes. Increasing the presence of WSNs in military and civil contexts leads to the necessity of security.

Necessarily, sensor nodes have not predetermined and certain place. Such a property allows us to release them in dangerous or inaccessible places.

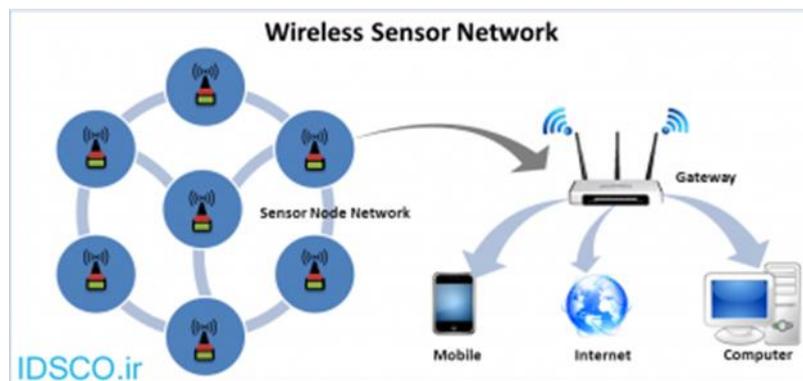


Figure 1. Nodes in a WSN

Protocols and algorithms of sensor networks should have self-organization capabilities. Each sensor node has a processor on its board. Instead of sending all raw information to the center or a node in charge of information processing and concluding, the sensor node firstly performs a series of elementary and simple processes on its obtained information and then, it sent the

semi-processed data. Although each sensor has a slight ability on its own, the combination of hundreds of sensor nodes provides new facilities. WSNs, indeed, have the power of applying a great number of small nodes which are able to be combined and organized. They are employed in various cases such as simultaneous routing, environmental conditions surveillance, and surveillance the health of structures, or the equipments of a system.

\* Corresponding Author  
Davoud Yazdanpanah

### THE GENERAL PROPERTIES OF A SENSOR NETWORK

Pair-to-pair network protocols create a mesh like communication service to transmit information among thousands of small devices through multi-mesh method. Adjustable architecture of mesh allows adjusting with new nodes to coverage a greater geographical area. Additionally, the system can automatically compensate one or more nodes. Unlike conventional wireless networks, in WSNS, all nodes are not required to directly communicate with the nearest power control tower or base station. But, sensors are divided into

clusters such that each cluster selects a header cluster or parent.

Each sensor in the network has a sensor area which fully surrounds that area. Although full coverage of the region is highly considered by sensors, some points may be not covered by any sensor. These points are called coverage holes.

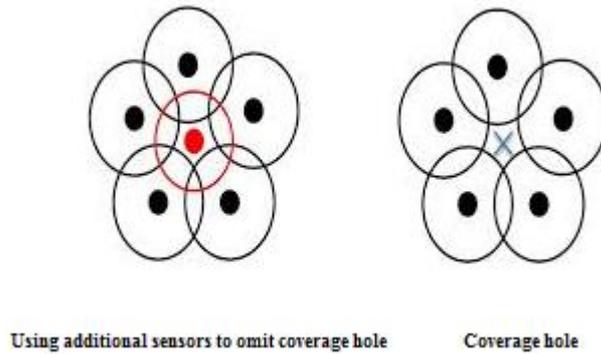


Figure 2. Schematic of coverage hole and the way of its omission

Enduring sensor nodes failure should not have any effect on the general function of the network. Therefore, enduring failure can be introduced as “the ability of maintaining operations of network in spite of the failure of some nodes”. Expansion capability of a network should be designed in such a way that it can actualize high density of sensor nodes as well. This density can vary from a few nodes to several hundred nodes in a region. Since sensor networks have been consisted of a large number of sensor nodes, the cost of a node is highly important to estimate total cost of the network.

**SECURITY REQUIREMENTS AND VARIOUS TYPES OF SENSOR NETWORK ATTACKS**

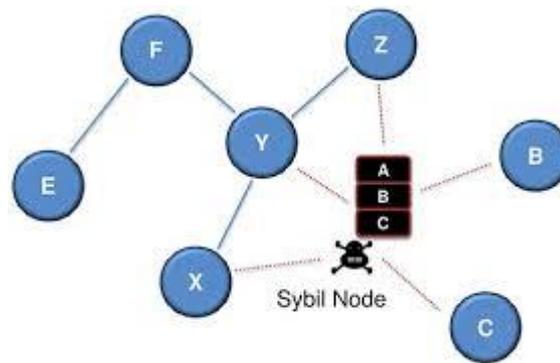
Data reliability, data integrity, data freshness, accessibility, self-regulation, secure establishment, using SeR-LoC (Secure Range-Independent Localization), system identification, etc.

Sybil attacks can be easily implemented in wireless sensor networks since sensor nodes have been distrib-

uted in an environment and communicate with each other through radio waves. The same capability provides this possibility for hackers’ attack.

Sybil attacks are regarded as a new threat for wireless sensor networks. In such attacks, a malicious node deceives network nodes by creating fake identities for itself [1-2]. These attacks can disturb operations such as routing, voting, data integration, nodes’ validity evaluation, fair resources allocation, and misbehavior detection [3]. Voting-based mechanisms lose their efficacy since some nodes are fake and their resulted information cannot be trusted [4].

Information security is highly important in some systems. For example, information confidentiality and security is very important where sensors gather medical information or military activity of tanks. Sybil attacks are regarded as the most important attacks in WSNs since they can provide the necessary context for many other attacks [5]. Further, they target control traffic attack and cause extensive damages.



**Figure 3. Sybil attacks modes**

With respect to the simplicity of implementing such attacks and information sensitivity in such networks, it is crucial to present strategies for detecting and coping with these attacks. In these strategies, processing, memory and power of WSNs should also be considered to be practically used in these networks.

To defend against Sybil attacks, we should legitimize the identity of each node presented by physical node. To this end, there are two ways. The first way is "direct confirmation" in which a node directly investigates the validity of another node's identity. The second way is "indirect confirmation" in which actualized nodes are allowed to guarantee or deny other nodes.

In the following, the methods proposed to detect Sybil attacks in wireless sensor networks are discussed and the best method is evaluated in a case study.

### **SYBIL ATTACKS**

Douceur claimed that under such distributed computational environment, a device can easily adopt several identities and it is due to the lack of a central and reliable power. In the following, there are various solutions proposed to detect Sybil attacks and omit them at network level.

- Encrypting and authentication
- Received information methods
- Intelligent methods
- Received Signal Strength Indicator (RSSI) [7]

### **ENCRYPTING AND AUTHENTICATION**

In a symmetric encryption mechanism, each node has a unique key with sump. Whenever two nodes have information to be exchanged, they firstly communicate with sump and announce their willingness to communicate. Sump investigates the identity of the two nodes through their symmetric keys and then, sends a shared key for both of them to allow them to directly communicate with each other. Reversely, when asymmetric encryption methods are used, public and private keys are firstly distributed among network nodes and then, digital signature is created [4]. Public encryption key is not computationally affordable for small

wireless sensors. Public encryption key or message identity determination in sensor nodes take just a few seconds [6]. Public Key Systems consume more memory compared to symmetric key systems. Moreover, they significantly increase message size. Accordingly, Public Key Systems significantly increase energy consumption and band width. Therefore, most of available encryption solutions for wireless sensor networks are based on symmetric key systems. However, key distribution is regarded as an important challenge in symmetric key systems [5].

Karlof and Wagner discussed the relative advantages of symmetric and asymmetric encryption techniques to protect wireless sensor networks against Sybil attacks [7]. They asserted that wireless sensor networks are susceptible to be subjected to Sybil attacks due to their distributed and unreliable environment. To defend against this attack, encryption keys and authentication mechanisms of nodes have been proposed. Due to the limitations of sensor nodes in saving and computational resources, it is not an appropriate method. On the other hand, using encryption keys cannot always cause to detect and prevent Sybil attacks. Newsome et al. proposed several methods including Radio Resources Test (RRT) and a Random Key Pre-distribution to protect wireless sensor networks against Sybil attacks. The mechanism of RRT is based on the assumption that nodes in a network cannot be simultaneously transmitted on more than one channel. When a node tends to see whether it has been the victim of a Sybil attack or not, it allocates a unique channel to each of its neighbors and asks them to disseminate a verification message on the allocated channels in a certain time. Then, the so called group randomly sets its receiver on one of the channels and waits to receive verification message. If no verification message is received, the group is suspicious. It is due to the fact that malicious node cannot simultaneously send verification message for all its fake identities on several channels. Repeating this trend, all fake nodes can be detected with a high probability. In this method, RKP of each node randomly selects  $k$  keys from a large tank with  $m$  keys in such a way that both nodes have one shared key certainly. Then, the identity of each node is combined with the identity of set of the selected keys and unique identi-

ties are produced. Therefore, each node can be identified and authenticated by confirming some or all their keys.

To prevent Sybil attacks, symmetric key encryption can be employed [8]. In this method, Zhang et al. used one of the important features of Merkle Hash Trees such that each node of leaf can be verified and confirmed providing that the amount of its parent is predetermined. Moreover, this feature is employed in another method in order that each network node can investigate and confirm the identity of other network nodes [9]. This method is efficient only in wireless sensor networks with small scale. Authentication methods often need to a large empty memory to save necessary identity information (e.g. shared encryption keys, identities, etc.) and complex processing. Additionally, if an attacker can intrude authentication mechanism, the general integrity of protective mechanism is disappeared [4].

#### **METHODS BASED ON INFORMATION RECEIVED FROM NODES**

In another method, to cope with Sybil attacks in wireless sensor networks, Su et al. investigated nodes' identity through analyzing the information of neighboring nodes of each node [4]. This method benefits from the reality that each malicious node offers a large number of fake identity to present a mechanism to protect wireless sensor networks against Sybil attacks. In the method, the assumption of networks with high density of nodes has been observed. The probability of the fact that two different nodes have exactly the same neighboring set is very low. In Sybil attacks, the faked nodes have similar sets of neighbors since all of them are related to a physical node, i.e. malicious node. Accordingly, the presence of malicious node can be detected through investigating neighboring nodes of victim node or investigating whether some of these nodes have similar neighboring or not (therefore, nodes are Sybil). They evaluated the feasibility of their method using both mathematical rules and numerically. They also empirically evaluated its validity using 8 groups (Tmote sky). The mechanism of defense is performed by a normal node suspicious to be victim. The considerable fact of the method is that the proposed method, instead of attempting to inquire each node, relies on a simple process of data gathering and analysis. Accordingly, this strategy prevents the risk of intentional wrong response and deceiving system's detection by malicious node. In another mechanism, improving their method, they asserted that if malicious node can be omitted, this node will not be effective anymore and the rest of victim node's neighbors will be normal node. Since setting communication range of sensor nodes are widely performed [23-24], this method has been used in this mechanism as well. Decreasing communication range of victim node is continued as far as malicious node is placed out of this range. Therefore, malicious node loses its effect and the number of

wrong detections is decreased. They continued to their work in the reference [25].

In his dissertation, Bhuse proposed two methods including Mutual Guarding (MG) and SRP to detect Sybil attacks. These two methods complement each other [26]. MG method is used when malicious node possesses the identity of one of neighboring nodes. Two nodes which are in communication range of each other can receive packets sent by another node. One malicious node placed in the common area of the two nodes cannot foist itself instead of each of these nodes since it is detected by them. SRP method is applied for MAC protocols that prevent collision through the exclusive access to channel. This method is appropriate when malicious node possesses an identity which is not present in its neighboring. Then, Sybil attack is detected through information exchange regarding the number of received packets of each node and comparing the number of sent and received packets.

#### **INTELLIGENT METHODS**

Banerjee et al. presented an intrusion detection mechanism based on ant's colony for wireless sensor networks [27]. Zhang et al. also attempted to decrease the effects of Sybil attacks on wireless sensor networks through ant's colony algorithm. In a network with Sybil nodes, Sybil node can be connected to normal nodes of network and accordingly, an edge is made between Sybil node and normal node. Using the nature of ants' colony algorithm, the number of malicious edges can be decreased [28]. Quercia et al. proposed a non-focused method to detect Sybil attacks in networks with mobile nodes. In their method, each node of two sets consisting of information related to nodes are gathered and maintained. One set constitutes friend network and another one consists attackers' network. The first set includes reliable nodes and the second set includes nodes to which nod suspect [29].

#### **ROUTING-BASED METHODS (RECEIVED SIGNAL)**

Demirbas and Song suggested using received signal strengths indicator (RSSI) to detect Sybil attacks [11]. Receiving a message from a new transmitter, node computes RSSI of that message. The computed RSSI, then, is ordered through the identity of the message transmitter (existing in the message) and saved in a search table. If in the future, node of another message is received with the same RSSI but a different transmitter identity, the incidence of a Sybil attack is announced.

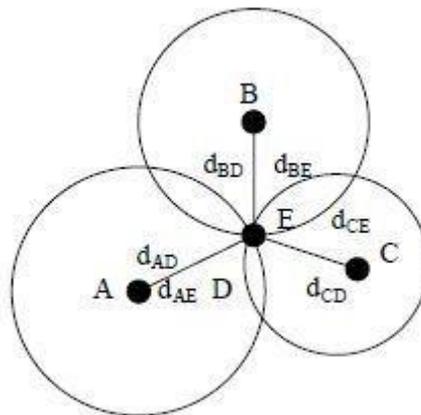
Zhong et al. also proposed to employ RSSI ratio to detect transmitter place through four surveillance nodes [12]. The routing algorithm proposed in this research can be used to detect Sybil attacks. Such that, receiving a message, the four surveillance nodes compute transmitter place and relate the resulted position with transmitter identity. Receiving a message with a new identity, then, transmitter place is computed and in

case of any similarity, Sybil attack is announced. It should be noted that it is very difficult and unnecessary to compute place. In fact, attack can be detected through computing and recording RSSI rate for received messages. Therefore, they use two receivers and RSSIs' ratio in their study.

Wang et al. suggested a similar mechanism to detect Sybil attacks in cluster-based wireless sensor networks [13]. They implemented channel model in which the effect of errors due to fading and path loss in communication channels of wireless sensor networks has been investigated.

They, then, proposed a combinational method to detect Sybil attacks. The proposed method detected attacks with respect to RSSI received by nodes and considering information provided and sent by network

nodes. They also presented a TDOA-based mechanism to detect Sybil attacks in cluster-based wireless sensor networks [14]. In this method, there are three guide nodes in each cluster. Sensor nodes within a cluster are heard by these three nodes. Guide nodes are informed about their place (for example, through GPS system). Sending message by nodes, TDOA is computed between transmitter node and guide node. TDOA rate, then, is related with transmitter identity. When two different identities with similar TDOA rate are observed, a Sybil attack is identified. In another method, a range finding technique is used to detect Sybil attacks in wireless sensor networks. Since Sybil nodes are caused by a malicious node, they are placed in a physical place. Accordingly, the distance of these nodes (Sybil) from a series of nodes should be identical [15].



**Figure 4. A sample of Nodes' range finding ALGORITHM**

LV et al. proposed Cooperative RSS-based Sybil Detection (CRSD) method for wireless sensor networks that employed received signal power to measure the distance between two nodes [22]. With the help of several neighboring nodes (the capability of nodes' cooperation), this method computes the distance between the considered node and these nodes. In this method, it is assumed that transmitting ability is identical and constant for all nodes (normal and malicious). All Sybil nodes have common physical place [11]; therefore, this method uses the place of nodes and RSS to detect Sybil attacks. To detect attack, a node puts those nodes with the identical distance to this node and similar RSS level in a group. Those nodes put in a group are Sybil nodes.

#### CASE STUDY

We conclude the discussion with a case study on an operating packet with a function called Detect which is in charge of detecting Sybil attack. Finding nodes suspicious to Sybil, this function puts them in a list whose algorithm will be introduced in the following. Here, SrcId and DstId fields are in charge of saving source and destination nodes in transmitting from one node to neighboring node.

The presented algorithm includes two phases of network preparation and network maintenance. In preparation phase, nodes are uniformly distributed and placed in network range. In this phase, base station randomly sends reliable nodes of the station based on a desirable percentage. After receiving operating packet, these nodes are selected as operating node. In maintenance phase, neighbors identified as attack agent are omitted. This process is performed during several stages. In each round, nodes disseminate a packet to construct a neighboring matrix and find neighbors with frequency range.

After finding neighbors of each node, every entry of neighboring matrix includes identities of nodes of neighbor 1. Under these conditions, truthtbit and agentbit related to neighbor are in false form in table. As finding neighbors, single-nodes save a memory of visited nodes. After finding neighbors and collecting memories related to that round, each node creates a packet called Msg including collected information as well as information of node entailing identity, place and so forth.

Detection algorithm is as following:

```

1- listmsg ← Receive-from-neighbors ();
2- foreach (msgi, msgj) listmsg do
3- if msgi.pos ==msgj.pos then
4- if msgi.id !=msgj.id then
5- Raise-alarm ();
6- if Check (msgi. History, msgj. History) == false then
7- Raise-alarm ();
    
```

**ATTACK DETECTION**

In this method, in each round, all operating nodes compare themselves with each other through recalling msg detection function existing in its list. This comparison is performed such that the information of msg transmitters is firstly compared. The information of transmitter node, then, is compared with the memory collected by other nodes. If more than one node is observed in a place with one round number, that node is put as Sybil attack to that agent and makes truttbite agent for all nodes existing in Lid list false. In this method, Ad Hoc on Demand Distance Vector (AODV) protocol is used for routing. Also, to prevent collision in Medium Access Control (MAC), CSMA/CA protocol has been employed [12]. Collision is prevented to improve the efficiency of CSMA. It works in such a way that if a node is transmitting information, another node will not be allowed to transmit; therefore, collision is minimized.

In the following, two series of simulations have been performed. One series of simulations includes only AODV protocol without any security mechanism and the second series of simulations, the presented mechanism has been used. All the experiments have been done in an environment of 200 200 m<sup>2</sup>. The experiments include several simulation implementations and in each simulation, implementation time has been considered 20 minutes. The number of nodes is 100. In each implementation, the number of Sybil nodes is 5 and these nodes have been uniformly distributed.

**OUTPUT RESULTS**

**THE NUMBER OF PACKETS DELIVERED TO INVASIVE NODES**

The number of packets delivered to invasive nodes is the number of packets delivered to malicious nodes. In this case, it has been assumed that packet is disappeared in network when it arrives to malicious nodes. PL rate refers to the number of packets delivered to malicious relative to total packets transmitted in the network. Figure 5 presents diagrams related to PL of the network for the number of various malicious nodes (5, 10 and 15) with different memory sizes (H) (10 and 15) compared to AODV protocol. As it is observed, PL rate in the proposed method (H=15) is less than the rest. It is due to the fact that more memory is maintained and accordingly, malicious nodes are identified earlier and omitted from neighboring list. Also, AODV protocol has greater number of PI since no security mechanism has been prepared in its.

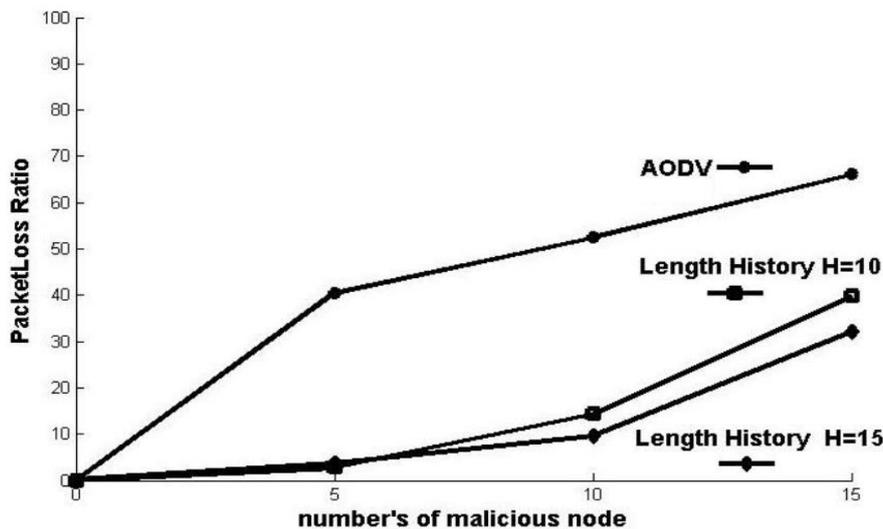


Figure 5. Packet loss ratio to malicious nodes

**OVERHEAD DUE TO ADDITIONAL MESSAGES**

Overhead due to additional messages exchanged between nodes is important due to using mobile agents to detect attack detection. To compute this rate, the number of the exchanged mobile operating packets to total exchanged packets of the network is computed. As shown in Figure 6, AODV protocol has a less and

constant overhead rate. However, firstly, higher mobile operating packets are exchanged in the network and this magnitude is gradually decreased. The reason of such decrease is that after identifying reliable nodes, the number of ordinary nodes exchanged between nodes to operating packet is increased. As a result,

operating packet use ration to total packets is decreased.

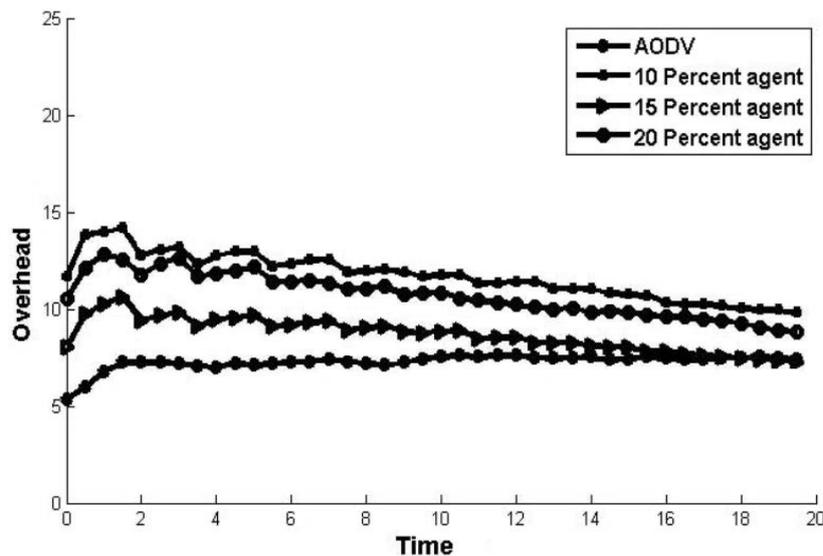


Figure 6. Overhead amount due to the performed simulation

## CONCLUSION

In Sybil attacks, a destructive node creates several fake identities for itself. Deceiving network nodes, this node disturbs operations such as voting, data integration, fair resources allocation, and anomaly detection. This fact, in its own, is a serious threat for WSNs. Methods that are proposed for wireless sensor networks should consider the limitations of these networks in processing resources, memory and power. Most of methods ignore these limitations to detect Sybil attacks in WSNs.

It can be stated that encryption and authentication-based methods are not appropriate methods due to their need to heavy processes. Additionally, in these methods, after intrusion to authentication mechanism, the integrity of authentication mechanism is disappeared and entire the network is at risk. Intelligent methods are regarded as new methods for attacks detection. These methods are appropriate when they do not lead to processing overhead. Localization-based methods, sometimes, require additional hardwares such as GPS and surveillance nodes, leading to the increase of sensor network cost and energy consumption. Another method is the method based on information received from nodes. The mentioned methods can be useful to detect attacks if the volume of transmitted and received information on the network is reasonable. High volume of exchanges causes communication overhead and the increase of energy consumption.

In the present paper, we employed a detection mechanism for Sybil attacks in wireless networks. The suggested method omits invasive nodes from neighboring list of each node through using memory gathered by

each node and mobile agent. Doing so, it prevents using them for routing. Through falsing the validity related to neighboring table of nodes, each malicious node will be omitted. Agent is assembly code segment that detects malicious nodes using the presented algorithm. Therefore, secure routing is achieved.

## REFERENCES

- [1] J.R. Douceur, "The Sybil attack," in Proc. of the International Workshop on Peer-to-Peer Systems, March 2002, pp. 251-260.
- [2] Z. Su, C. Lin, F. Ren, X. Zhan, "Security mechanisms analysis of wireless sensor networks specific routing attacks," in Proc. of 2006 1st International Symposium on Pervasive Computing and Applications, pp. 579-584.
- [3] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis and defenses," in Proc. of 2004 International Symposium on Information Processing in Sensor Networks, pp. 259-268.
- [4] K. F. Ssu, W. T. Wang, W. C. Chang, "Detecting Sybil Attacks in Wireless Sensor Networks Using Neighboring Information", Computer Networks, vol. 53, no. 18, pp. 3042-3056, Dec. 2009.
- [5] S. Misra, I. Woungang, S. C. Misra, Guide to Wireless Sensor Networks, Springer, 2009, pp. 491-512.
- [6] D. J., Malan, M., Welsh, M., Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, pp. 71 - 80, 2004.

- [7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proc. of 2003 IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113–127.
- [8] Q. Zhang, P. Wang, D.S. Reeves, P. Ning, "Defending against Sybil attacks in sensor networks," in Proc. of 2005 IEEE International Conference on Distributed Computing Systems Workshops, pp. 185–191.
- [9] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247-260, Feb. 2006.
- [10] D., Liu, P., Ning, "Establishing pairwise keys in distributed sensor networks," Proceedings of the ACM Conference on Computer and Communications Security, pp. 52–61, October 2003.
- [11] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks," in Proc. Of International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 564–570, 2006.
- [12] S., Zhong, L., Li, Y. G., Liu, Y. R., Yang, "Privacy-preserving location based services for mobile users in wireless networks", Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2004.
- [13] J., Wang, G., Yang, Y., Sun, S., Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2684-2687, 2007.
- [14] W. Mi, L. Hui, Z. Yanfei and C. Kefei, "TDOA-based Sybil attack detection scheme for wireless sensor networks," Journal of Shanghai University (English Edition), Vol. 12, No.1, pp 66-70, 2008.
- [15] R., Xiu-li, Y., Wei, "Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network" 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1 – 4, 2009.
- [16] Z., Zhi-Guang, "A WSN Node Ranging Method Based on Phase Difference Measurement," Chinese Journal of Sensors and Actuators, Vol. 20, No. 12, pp. 2728-2732, December 2007.
- [17] J., Yang, Y., Chen, W., Trappe, "Detecting sybil attacks in wireless and sensor networks using cluster analysis," IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 834 – 839, October 2008.
- [18] G., Lee, J., Lim, D., Kim, S., Yang, M., Yoon, "An Approach to Mitigating Sybil Attack in Wireless Networks using ZigBee," International Conference on Advanced Communication Technology, pp. 1005 – 1009, April 2008.
- [19] F., Amini, J., Mistic, H., Pourreza, "Detection of Sybil Attack in Beacon Enabled IEEE802.15.4 Networks," International Conference on Wireless Communications and Mobile Computing, pp. 1058 – 1063, August 2008.
- [20] A., Flammini, D., Marioli, G., Mazzoleni, E., Sisinni, A., Taroni, "Received Signal Strength Characterization for Wireless Sensor Networking," Proceedings of the IEEE Instrumentation and Measurement Technology Conference, pp. 207 – 211, April 2006.
- [21] J. F., Kurose, K. W., Ross, "Computer Networking: A Top-Down Approach Featuring the Internet," May 2004.
- [22] S., Lv, X., Wang, X., Zhao, X., Zhou, "Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", International Conference on Computational Intelligence and Security, pp. 442 – 446, December 2008.
- [23] S., Lin, J., Zhang, G., Zhou, L., Gu, T., He, J.A. "Stankovic ATPC: adaptive transmission power control for wireless sensor networks," Proceedings of the International Conference on Embedded Networked Sensor Systems, pp. 223–236, November 2006.
- [24] C., Song, M., Liu, J., Cao, Y., Zheng, H., Gong, G., Chen, "Maximizing network lifetime based on transmission range adjustment in wireless sensor networks," Special Issue of Computer Communications on Heterogeneous Networking for Quality, Reliability, Security, and Robustness, Vol. 32, No. 11, pp. 1316–1325, 2009.
- [25] W. T., Wang, K. F., Ssu, W. C., Chang, "Defending Sybil Attacks Based on Neighboring Relations in Wireless Sensor Networks," Security and Communication Networks, Vol. 3, No. 5, pp. 408-420, 2010.
- [26] V. S, Bhuse, "Lightweight Intrusion Detection: A Second Line of Defense for Unguarded Wireless Sensor Networks." Doctoral Dissertation, Western Michigan University, January 2007.
- [27] S., Banerjee, C., Grosan, A., Abraham, P. K., Mahanti, "Intrusion Detection on Sensor Networks Using Emotional Ants." International Journal of Applied Science and Computations, Vol. 12, No. 3, pp. 152-173, 2005.
- [28] B., Zeng, B., Chen, "SybilACO: Ant colony optimization in defending against Sybil attacks in the wireless sensor network", International Conference on Computer and Communication Technologies in Agriculture Engineering, pp. 357 – 360, August 2010.

- [29] D., Quercia, S., Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," Proceedings of IEEE INFOCOM, pp. 1-5, May 2010.