VOL 2 (2018) NO 3

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Sybil Node Detection in Mobile Wireless Sensor Networks Using Observer Nodes

Mojtaba Jamshidi [#], Milad Ranjbari [*], Mehdi Esnaashari [**], Nooruldeen Nasih Qader [***], Mohammad Reza Meybodi [****]

[#]*Department of Electrical, Computer and IT Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran*

[*]*Department of Computer Engineering, Arak Branch, Islamic Azad University, Arak, Iran*

[**] *Faculty of Computer Engineering, K. N. Toosi University of Technology, Tehran, Iran*

[***] *Computer Science Department, University of Human Development, Iraq*

[****] *Computer Engineering and Information Technology Department, Amirkabir University of Technology, Tehran, Iran*

E-mail: jamshidi.mojtaba@gmail.com, miladranjbari@gmail.com, esnaashari@kntu.ac.ir, nooruldeen.qader@uhd.edu.iq, mmeybodi@aut.ac.ir

***Abstract*— Sybil attack is one of the well-known dangerous attacks against wireless sensor networks in which a malicious node attempts to propagate several fabricated identities. This attack significantly affects routing protocols and many network operations, including voting and data aggregation. The mobility of nodes in mobile wireless sensor networks makes it problematic to employ proposed Sybil node detection algorithms in static wireless sensor networks, including node positioning, RSSI-based, and neighbour cooperative algorithms. This paper proposes a dynamic, light-weight, and efficient algorithm to detect Sybil nodes in mobile wireless sensor networks. In the proposed algorithm, observer nodes exploit neighbouring information during different time periods to detect Sybil nodes. The proposed algorithm is implemented by J-SIM simulator and its performance is compared with other existing algorithm by conducting a set of experiments. Simulation results indicate that the proposed algorithm outperforms other existing methods regarding detection rate and false detection rate. Moreover, they also showed that the mean detection rate and false detection rate of the proposed algorithm are respectively 99% and less than 2%.**

***Keywords*— Wireless sensor networks, Sybil attack, mobile node, observer node.**

I. INTRODUCTION

Type wireless sensor networks are ad hoc wireless networks, which contain hundreds to thousands of cheap sensor nodes. Sensor nodes have constraints including energy, memory, radio range, and power computation. According to these constraints, the broadcast nature of wireless communications, and the lack of resistance of sensor nodes against adversary tampering, security has become an important and challenging issue in these networks [1, 2].

Sybil attack [3] is one of the important attacks affecting the network layer (routing). In Sybil attack, the adversary captures a legitimate node in the network and reprograms it (as a malicious node) or inserts a legitimate node as a malicious one in the network. After deployment in the network operational environment, this malicious node propagates several IDs (from here on referred to as "Sybil nodes"), which are fabricated by the adversary or stolen from legitimate nodes in other areas of the network. When this malicious node simultaneously propagates several IDs, this attracts a lot of traffic, since legitimate neighbour nodes assume that each ID (Sybil node) corresponds to an individual physical node; whereas, all the IDs (Sybil nodes) correspond to one and only one hardware node. Therefore, this attack can significantly disrupt routing protocols and even operations, including voting, misbehavior detection, data aggregation, and reputation evaluation [3-5].

We must note that many algorithms [6-16] have been proposed to detect Sybil nodes in static wireless sensor networks, which cannot be integrated into mobile ones. The reason is that most of these algorithms are based on node positioning or identify Sybil nodes based on RSSI or neighbor cooperation; however, the mobility of nodes (Sybil and non-Sybil) in mobile wireless sensor networks can disrupt the execution of these algorithms.

Also, in [17-19] algorithms are proposed for detecting Sybil nodes in mobile sensor networks. In [17], a centralized

algorithm is proposed which includes 3 phases of clustering, selecting nodes in the vicinity of Sybil node, and routing procedures. So, it cannot be a proper algorithm. In [18], another centralized algorithm is proposed which is based on nodes' registration in a base station. This algorithm is based on a base station so faces with scalability issue. In [19], our previous algorithm is proposed which is uses a distributed labeling mechanism to assigned bit label to nodes based on their movement. This algorithm requires exchanging so many messages between the watchdog nodes which increases communication overheads and power consumption as a result. Added to this, the algorithm has a relatively low Sybil nodes detection rate.

Therefore, this paper proposes a novel light-weight algorithm to detect Sybil nodes in mobile wireless sensor networks using observer nodes. The proposed algorithm is not based on node positioning, RSSI, or authentication methods and only detects Sybil nodes by monitoring the network traffic.

The rest of this paper is organized as follows. Section II presents previous work, system assumption, attack model, symbols, and the proposed algorithm. Section III discusses the performance evaluation and simulation results. The paper is concluded in Section IV.

II. Material And Method

In this section, we first present some existing algorithms which are proposed to defend against Sybil attack in wireless sensor networks. Then, we present the preliminaries of the proposed algorithm, including assumptions, attack model, and symbols. Finally, the proposed algorithm is presented.

A. *Related Work*

Sybil attack was first introduced by Douceur in [3] where it is noted that peer-to-peer networks are vulnerable to this attack. In [4], Karlof stated that the attack can affect routing protocols of sensor networks. First, Newsome et al. [6] analyzed Sybil attack to wireless sensor networks systematically and introduced mechanisms like key pre-distribution, radio source test, identity registration, and remote authentication code to deal with the attack. In [7], an RSSI-based locating algorithm is proposed that uses the RSSI proportion of several receivers to estimate the location of nodes in a network. In [8] and [9], the locating mechanism proposed in [7] is used for detecting Sybil nodes. Algorithm [8] uses four location-aware nodes (track¬ing nodes) capable of hearing packets throughout the network. Tracking nodes cooperate to locate any nodes sending packets. This is sufficient to detect Sybil nodes since all of them positioned in nearby locations. RSSI-based algorithms also cannot be an appropriate solution since radio signals are prone to be interfered with by the environment, as a result, the detection precision of such algorithms is affected.

In [10-13], algorithms are proposed for detecting Sybil nodes in cluster-based sensor networks. Algorithms proposed in [14-16] use the concept of common neighbors to detect Sybil nodes. In [17], another algorithm is proposed for detecting Sybil attack to multicast routing protocols based on geographic location. In [18], a method is developed which collects routes' information using Swarm Intelligence algorithm during network operation and detects Sybil nodes through their energy changes in the course of network activity. Also, in [19-21], some other algorithms are proposed for detecting Sybil nodes in mobile sensor networks, the mechanism, and limitation of which are explained in the previous section.

In [22], a mechanism based on evaluating trust values of neighbor nodes is proposed to detect Sybil nodes in wireless sensor networks. The nodes with the trust values less than a threshold value are detected as Sybil nodes. In [23], a message authentication algorithm is proposed for detecting Sybil nodes in wireless sensor networks. This algorithm uses message authentication and passing procedure for authentication prior to communication. In [24], a Random Password Generation (RPG) algorithm is proposed that analyze the traffic levels to defend against Sybil attack. In [25], a location algorithm is proposed that uses the characteristics of received signal powers of the nodes to detect Sybil nodes. In [26], a rule-based anomaly detection system is proposed which relies on an Ultra-Wide Band (UWB) ranging-based detection algorithm to defend against Sybil attack. In [27], a one-way key chain ID authentication algorithm is proposed to decrease the probability for attackers to lunch Replica and Sybil attacks which used elliptic curve discrete logarithm problem and node neighbor relationship to authorized nodes.

B. *System* Assumptions

In this study, it is assumed that the total number of nodes is N = SN + ON (SN is the number of normal sensor nodes and ON is the number of observer nodes). Observer nodes periodically monitor the network traffic and detect Sybil nodes. All sensor nodes (normal and observer) are randomly distributed in a two-dimensional region. Sensor nodes are mobile and move in the environment during the network lifetime according to mobility models, e.g. random waypoint. Nodes have a unique ID and are unaware of their location. Nodes communicate through a wireless radio channel and employ an Omni-directional mode broadcast. The radio range of all nodes is fixed and equal to r. moreover, it is assumed that if necessary, observer nodes utilize multi-hop reactive routing algorithms to make a route for them to communicate. Furthermore, it is assuming that normal sensor nodes are not tamper-resistant and an adversary can capture a node to access its confidential information and reprogram it. In contrast, it is assumed that observer nodes are tamper-resistant and adversaries cannot decrypt and reprogram them.

C. Attack *Model*

The attacked model considered in this study based on the taxonomies in [5] includes direct, simultaneous Sybil attack and fabricated IDs. It is assumed that the network is insecure and nodes may be captured by adversaries. A node captured by an adversary is called a malicious node and the rest are called normal nodes. Each malicious node propagates several IDs (Sybil nodes). Moreover, it is assumed that each malicious node propagates at least Tmin Sybil IDs. Similar to normal sensor nodes, malicious nodes are also mobile in the network environment. According to [9], the adversary can disrupt network operations in two ways using the Sybil attack. In the first case, the adversary captures a large number of nodes in the network, reprograms them as

malicious nodes, and re-injects them, such that each malicious node propagates few Sybil IDs (e.g. 2 or 3). In this case, security algorithms hardly detect Sybil nodes and even some methods, including [9], may not detect them. However, it is difficult and time consuming for the adversary to capture, decrypt, reprogram, and control a large number of normal nodes in the network. The second case is when an adversary captures a smaller number of normal nodes and reprograms them as malicious ones, such that each malicious node propagates a larger number of Sybil IDs.

Similar to [9], the proposed algorithm assumes that the adversary follows the second case. Similar to normal and observer nodes, malicious nodes are also mobile in the network environment. Moreover, it is assumed that at each stage of mobility and reaching a new location in the network, each node propagates a "Hello" message, route request, etc. this in fact is one of the requirements of mobile wireless sensor networks, so that each node can identify its current neighbours at any moment and if necessary, communicate or establish security keys with them, generate its routing table, etc. [15]. It is clear that in this case when each malicious node enters a new location in the network, it should transmit a "Hello" message, route request, etc. for all its Sybil IDs. (Simultaneous Sybil attack model [5]). The proposed algorithm uses this type of propagated messages to detect Sybil nodes.

D. *Symbols*

- *History*: a vector in the memory of each observer node to keeps necessary information about movements of normal nodes.
- *P*: the number of monitoring iterations of network traffic by observer nodes (the number of iterations in the first phase of the proposed algorithm)
- T_{min}: minimum number of Sybil *IDs* propagated by a malicious node.
- $\{S_1^m, S_2^m, ...S_j^m\}$: Sybil *IDs* propagated by malicious node m.
- *Suspicious_list*: a list in the memory of observer nodes to temporary store the *ID* of suspected Sybil nodes.
- Set_u^i : set number *i* in the *suspicious_list* of observer node *u*.
- $Sybil\_list_u$: a list containing the Sybil node detected by observer node *u*.
- *d*: the diameter of the network.
- ϖ : the average number of neighbors of a node in the network.
- *ON*: the number of observer sensor nodes in the network.
- *SN*: the number of normal sensor nodes in the network.
- *N*: the total number of nodes in the network ($N = SN + ON$).
- *M*: the number of malicious nodes in the network
- S: the number of Sybil *IDs* propagated by each malicious node.
- *r*: radio range of the nodes.

E. *The Proposed Algorithm*

The main notion of the proposed algorithm is inspired by the number of node occurrences in the neighborhood of observer nodes. As it was mentioned, we have two types of sensor nodes in the proposed algorithm (normal and observer nodes). Normal sensor nodes perform the network mission, including collecting information, sending data to the base station, etc. and the observer nodes periodically monitor the network traffic and identify Sybil nodes. Fig 1 presents a flowchart of the proposed algorithm. The proposed algorithm consists of two phases. The network traffic monitoring phase and the Sybil node detection phase, which are both performed by observer nodes. In what follows, these two phases are explained.

Phase 1: after deployment in the network environment, sensor nodes begin to transmit packets (packet containing the data, "Hello" packet", route request packet, etc.) and move in the corresponding environment. Each observer node has a vector (with n entries) in its memory, called history, which stores the occurrences of other nodes in its neighborhood. Accordingly, during each time period t, if a node like u appears in its neighborhood, each observer node adds a unit to the field corresponding to node u in its history vector. Time period t is selected large enough to allow observing the behavior of all Sybil IDs corresponding to a malicious node, including data transmission, "Hello" messages, route requests, etc. [19]. In other words, time distance t is selected large enough to reveal all Sybil IDs corresponding to their malicious node. Since after entering a new location in the network, all normal and Sybil sensor nodes send packets (e.g. "Hello" packet), if an observer node is present in that location, it records the entrance of new nodes to that location in its history vector. Therefore, after P time periods of network lifetime, observer nodes will contain the occurrences of other nodes in their neighborhoods in their history.

Phase 2: after running the first phase, in order to detect Sybil nodes, each observer node *u* navigates its history vector and generates distinct sets of node *IDs*, such that each set includes the *IDs* of nodes, which appeared for an equal number in the node *u*'s neighborhood. subsequently, the observer node stores the sets, whose members are larger or equal to T_{min}, as suspicious Sybil nodes in a list of sets, called *suspicious_list*. Since it is assumed that each malicious node propagates at least T_{min} Sybil *IDs*. Therefore, for each observer node, the *suspicious_list* contains sets, whose members are suspected to be Sybil. Assuming that malicious nodes *a* and *b* propagate Sybil nodes $\{S_1^a, S_2^a, ...S_i^a\}, \{S_1^b, S_2^b, ...S_j^b\} : i, j \geq T_{\min}$, since all Sybil nodes correspond to one malicious node, and thus, they move together, the occurrences of nodes $\{a, S_1^a, S_2^a, ...S_i^a\}$ will be equal in the neighborhood of observer node *u* (e.g. α times). Moreover, the occurrences of nodes $\{b, S_1^b, S_2^b, ...S_j^b\}$ will also be equal in the neighborhood of observer node *u* (e.g. β times). Therefore, all nodes $\{a, S_1^a, S_2^a, ...S_i^a\}$ are placed in a set and all $\{b, S_1^b, S_2^b, ...S_j^b\}$ are stored in another in the *suspicious_list* of observer node *u*. Moreover, there may be

some normal nodes, which have been present in the neighborhood of *u* for an equal number of times (e.g. α or β). Therefore, in addition to Sybil node *IDs*, sets in the *suspicious_list* of *u* will also contain the *IDs* of normal nodes. Accordingly, the false detection rate is increased if an observer node independently marks all *IDs* in its *suspicious_list* as Sybil nodes.

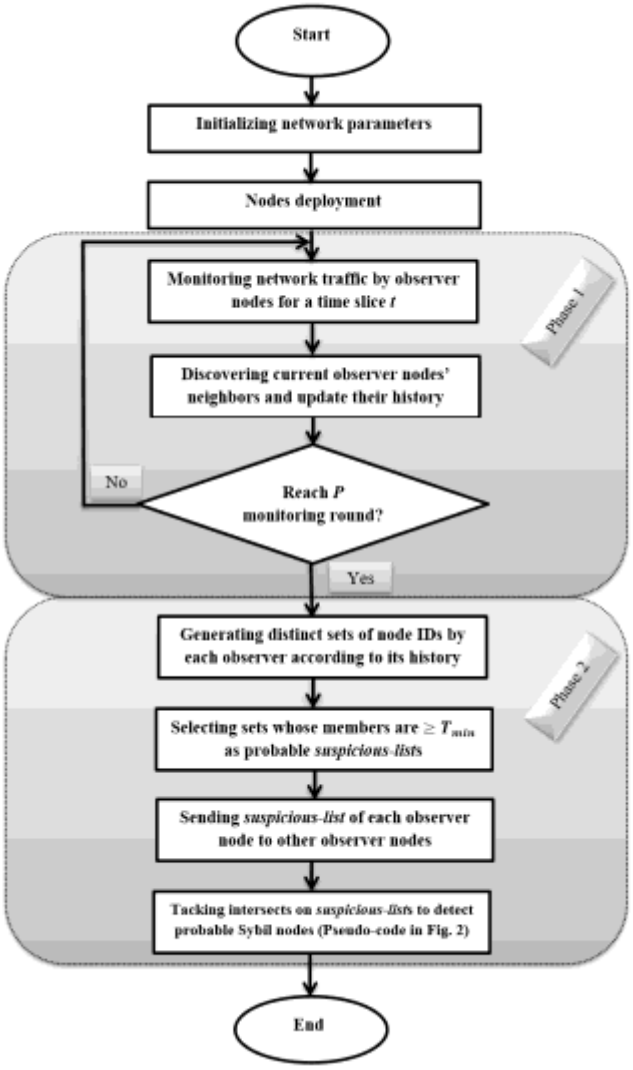

Fig. 2 Flowchart of the proposed algorithm

In order to increase detection accuracy, observer nodes cooperate to detect Sybil nodes. More specifically, observer nodes send their *suspicious_list*s to each other. They first utilize a multi-hop reactive routing algorithm, e.g. [22], to generate routes between themselves and then exchange their *suspicious_list*s through them. After receiving all *suspicious_list*s (from other observer nodes), an observer node begins to detect Sybil nodes. More specifically, each observer node intersects the *suspicious_list*s of other observer nodes and its own to mark Sybil nodes. The intersection operation is performed by each observer node *u* by navigating other sets in the *suspicious_list*s received from other observer nodes, e.g. Set_v^j, for each existing set in its own list, e.g. Set_u^i and inserting the *IDs* resulting from intersecting these two sets in Set_u^i, if the intersection of these two sets is larger or equal to $T_{\min}$. After this operation, if the number of remaining members in Set_u^i in larger or equal to $T_{\min}$, its content is added to the set of Sybil *IDs* of observer node *u* (called $Sybil\_list_u$). Node *u* repeats this operation for all sets in its *suspicious_list*. Finally, $Sybil\_list_u$ will contain the *IDs* that are detected as Sybil by *u*. Fig. 2 presents the pseudo-code for the main core of the second phase of the proposed algorithm.

```
node u for each Set_u^i in it's Suspicious_list Do
{
    for each node v Do
        for each Set_v^j in Suspicious_list_v Do
            if (Set_u^i ∩ Set_v^j ≥ T_min) then
                Set_u^i = Set_u^i ∩ Set_v^j
    if (Set_u^i ≥ T_min) then
        Sybil_list_u = Sybil_list_u ∪ Set_u^i
}
```

Fig. 3 Pseudo-code for the second phase of the proposed algorithm

III. RESULTS AND DISCUSSION

In this section, we first evaluate the overhead of proposed algorithm in terms of memory, communication, and computation. Then, we simulate the proposed algorithm and evaluate its detection rate through some experiments. We also compare its detection rate with the other existing algorithms.

A. Overhead Evaluation

Memory overhead: since the proposed algorithm is only executed by observer nodes, memory overhead only corresponds to those nodes and normal ones bear no overhead by the proposed algorithm. In the proposed algorithm, each observer node requires a space of order O(*SN*) to store the occurrences of other nodes in its history vector. Moreover, in the Sybil node detection phase (marking Sybil nodes), each observer node requires generating distinct sets of node *IDs* and temporary store its *suspicious_list* and those of other observer nodes in its memory to perform intersection on them. At this stage, memory overhead reaches $O(ON \times SN)$. However, since after detecting Sybil nodes, observer nodes free the space of *suspicious_list*s and distinct sets, the memory overhead imposed by the proposed algorithm on observer nodes can be considered of order O(*SN*). Since observer nodes are only responsible for monitoring and detecting Sybil nodes and no memory is consumed for other operations in the network, including data aggregation, clustering, etc., thus, they will have sufficient free memory to store the history vector.

Communication overhead: energy consumption of an algorithm is critical due to the limitation of sensor nodes' energy. Since sending packets consumes far much energy in comparison to other operations such as receiving or computing, therefore the number of transmitted packets imposed upon the network during execution of a certain algorithm is considered as a significant criterion. The first

phase of the proposed algorithm imposes no considerable communication overhead to the network and the only communication overhead of the proposed algorithm corresponds to sending *suspicious_list*s by observer nodes in the second phase. Each observer node should send its *suspicious_list* to other observer nodes in a multi-hop fashion. Assuming that the diameter of the network is *d*, each observer node should send its *suspicious_list* to other observer nodes by $(ON-1)\times d$ transmissions. Therefore, the total imposed communication overhead is $(ON\times(ON-1)\times d)$. We must note that the proposed algorithm will also have the communication overhead corresponding to running the reactive routing algorithm to find a route between observer nodes. Moreover, the number of observer nodes is very smaller than that of normal nodes in the network ($ON << SN$).

Computational overhead: the proposed algorithm imposes no computational overhead to the normal sensor nodes. In the first phase of the proposed algorithm, each observer node will have a computational overhead of $O(P\times N\times\varpi)$ to store information in its history vector. The reason is that during each iteration of the first phase of the proposed algorithm, for each of its current neighbours, e.g. a, the observer node navigates its history vector and adds a unit to the index corresponding to a. in the second phase, each observer node first navigates its history vector and creates distinct sets of node *IDs*, which is feasible with a time order of O(*N*) (having an auxiliary space of order O(*N*)). The observer node should then select suspicious sets from these distinct ones and add them to its *suspicious_list*, which is possible with a time order of O(*N*). Finally, the observer node should detect Sybil nodes according to its *suspicious_list* and those of other observer nodes and by performing the aforementioned intersection operation in fig. 1. Assuming that the *suspicious_list* of each observer node has *k* sets on average, thus, each observer node performs intersection and Sybil node detection in a time order of $O(k^2\times ON)$.

B. Simulation Results

The proposed algorithm was simulated by J-SIM simulation [28] and its performance was compared with other algorithms [9, 10, 15, 16, 21, and 23] by conducting a set of experiments. The evaluated measures are as follows.

Detection Rate: the percentage of Sybil nodes, which are detected by a security algorithm.

False Detection Rate: a percentage of normal nodes, which are falsely detected as Sybil nodes by a security algorithm.

It is assumed that the network consists of *N* sensor nodes, which are randomly scattered in 100×100 square meters. The operational area includes *M*=5 malicious nodes, which are randomly scattered in the network environment. Parameter T_{min} is set to 10. Each malicious node propagates *S* fabricated *IDs*. All nodes (normal and malicious) have the same radio range equal to 10 meters. Moreover, the mobility model considered in [29] is used to model the nodes` mobility in the network environment. In order to insure the credibility of results, each simulation is repeated 100 times and the final results are achieved by averaging these 100 repetitions.

Experiment 1: this experiment aims to evaluate the proposed algorithm regarding the detection rate of Sybil nodes. In this experiment, the number of sensor nodes is *N*=300, from which 5 are observer nodes (*ON*=5). Moreover, the number of Sybil *IDs* propagated by each malicious node is changed from 10 to 20 (with an increase step of 5). The detection rate of Sybil nodes by the proposed algorithm is evaluated for time periods of 25 to 300 and the results are presented in Fig. 4. Experiment results indicate that changing the number of Sybil *IDs* has no effect on the detection rate of the proposed algorithm and this measure is higher than 99% after 200 time periods.

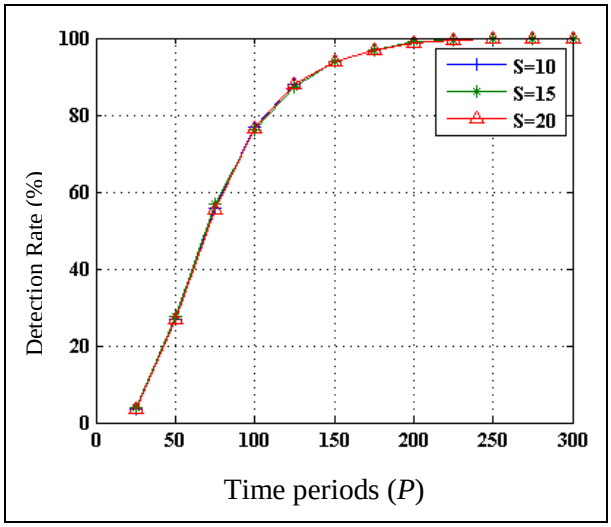

Fig. 4 Detection rate of the proposed algorithm for various rounds and Sybil identities

Experiment 2: this experiment investigates the effect of the number of observer nodes on the detection rate of the proposed algorithm. In this experiment, *S*=20, and *N*=300, the number of observer nodes is changed from 2 to 10 (with an increase step of 2), and its effect is evaluated on the detection rate of Sybil nodes during time periods 25 to 300. Fig. 4 presents the results of this experiment. As we can see, for different values of *ON* (the number of observer nodes), after 150 time periods, the detection rate of the proposed algorithm is higher than 90% and after 200 time periods, it is higher than 99%. The result of this experiment shows that the detection rate of Sybil nodes is increased by reducing the number of observer nodes and conversely, decreased by increasing their number. The reason is that observer nodes cooperate and perform an intersection operation on distinct sets (*suspicious_lists* of observer nodes) to detect Sybil nodes. Therefore, with a smaller number of observer nodes, the intersection of distinct sets will have a larger number of members, which increases both the detection rate and false detection rate (as experiment 3). Of course, after 200 time periods, the detection rate is higher than 99% for different numbers of observer nodes.

Moreover, Fig. 5 presents the performance of the proposed and other existing algorithms regarding detection rate. As we can see, the detection rate of Sybil nodes (on average) by algorithm [21] and the proposed algorithm is about 99%. Whereas, detection rates of other algorithms are less than 99%. However, algorithm [21] is only applicable in

static wireless sensor networks. Experiment results indicate the desirable performance of the proposed algorithm regarding the detection rate of Sybil nodes.

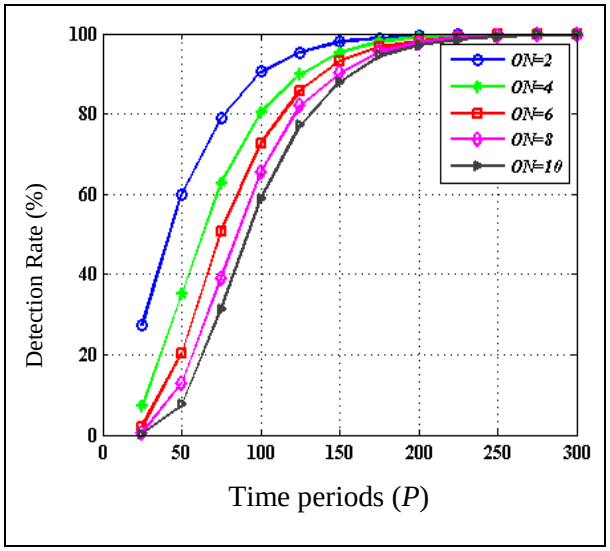

Fig. 5 The effect of the number of observer nodes on the detection rate of the proposed algorithm

Experiment 3: this experiment aims to evaluate the false detection rate of the proposed algorithm. The number of nodes in this experiment is also N=300. Moreover, the number of Sybil *IDs* propagated by malicious nodes is assumed S=20, observer nodes are changed from 4 to 10 (with increase step of 2), and its effect on the false detection rate of the proposed algorithm is evaluated in time periods 100 to 1000. Fig. 6 presents the experimental results. As we can see, a larger number of observer nodes reduces false detection rate, since observer nodes cooperate and intersect to detect Sybil nodes. Experiment results indicate that if ON=10, after 500 time periods, the false detection rate is about 5% and after 900 time periods, this measure is about 0%. Furthermore, Fig. 7 presents the false detection rate, on average case, of the proposed and the other algorithms. The average false detection rates of the algorithms in [26] and [28] are about 0%, algorithm [15] and the proposed algorithm are about 2%, and the other algorithms are more than 2%.

Experiment 4: This experiment examined the effect of the number of Sybil *IDs* issued by malicious nodes (S) on the false detection rate of the proposed algorithm. We set N=300 and ON=10 in the experiment, changed the number of Sybil *IDs* issued by any malicious node from 10 to 20 (with increment 2) and then evaluated its effect on the false detection rate of the proposed algorithm for the periods 100 to 1000. Fig. 8 depicts the results of the experiment. As demonstrated by the experiment results, false detection rate decreases with the increase of the number of the node Sybil *IDs* issued by malicious nodes. However, the reduced number of the Sybil *IDs* issued by malicious nodes led to the increased rate of the criterion. The reason may be that whatever the number of the Sybil *IDs* is less, more *IDs* may be wrongly detected as Sybil with regard to the form of intersecting and detection of the Sybil nodes that were described in the second phase of the proposed algorithm. However, the false detection rate for the state of $S>18$ may be 5% after 500 periods and less than 10% for the state of $S \geq 12$ after 1000 periods. Of course, the criterion rate would tend to zero for all values of $S \geq 10$ by increasing the number of periods. For instance, false detection rate for S= 18 and S=20 respectively would be 0.3% and 0.1% after 1000 periods.

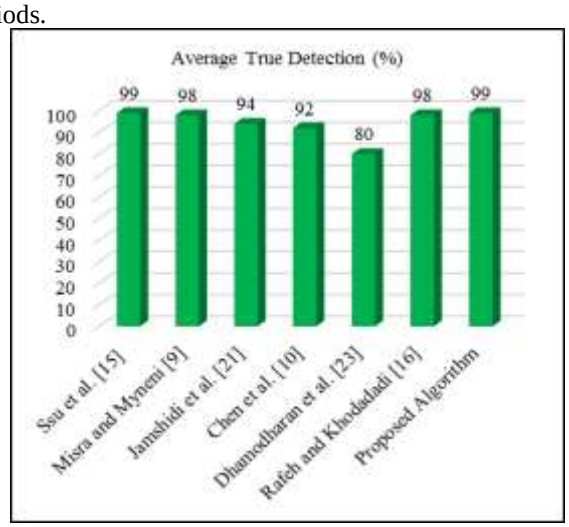

Fig. 5 Comparison of the proposed algorithm with the other existing algorithms in terms of average detection rate.

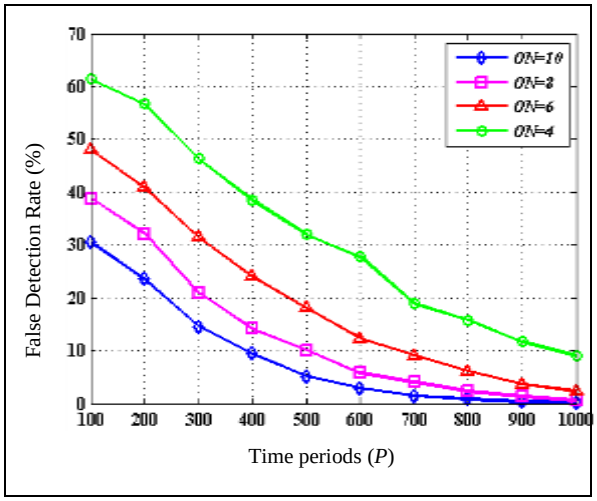

Fig. 6 The effect of the number of observer nodes on the detection rate of the proposed algorithm.

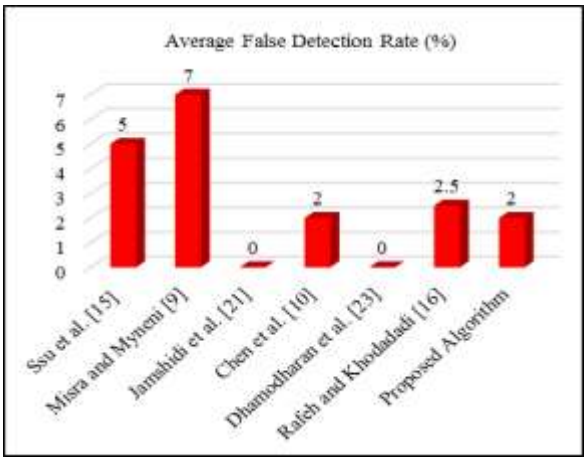

Fig. 7 Comparison of the proposed algorithm with the other existing algorithms in terms of average false detection rate.

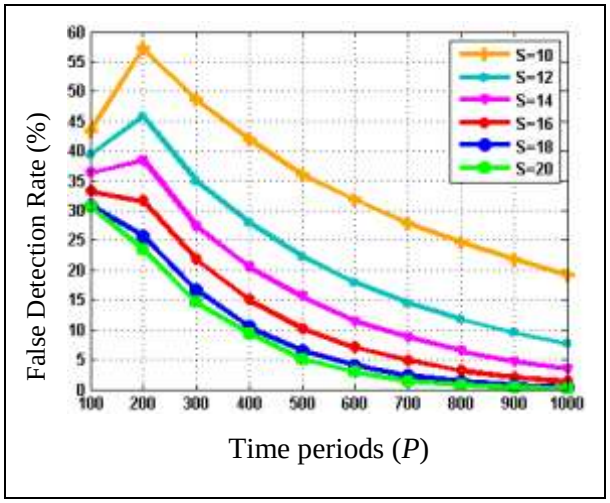

Fig. 8 The effect of parameter *S* on false detection rate of the proposed algorithm

IV. CONCLUSIONS

This paper proposed a distributive, light-weight, and efficient algorithm to detect Sybil nodes in mobile wireless sensor networks. In this algorithm, during different time periods, observer nodes store the occurrences of other nodes in a vector called history. In order to detect Sybil nodes, observer nodes cooperate and identify Sybil node IDs based on the content of history vectors. The proposed algorithm was simulated and its performance was compared with that of other algorithms [9, 10, 15, 16, 21, and 23] by conducting a set of experiments. Experiment results indicate the desirable performance of the reposed algorithm regarding detection rate and false detection rate.

REFERENCES

[1] A. Rathee, R. Singh, and A. Nandini. "Wireless Sensor Network-Challenges and Possibilities." *International Journal of Computer Applications*, vol. 140, no. 2, 2016.

[2] A. R., Dhakne and P. N. Chatur. "Detailed Survey on Attacks in Wireless Sensor Network." *In Proceedings of the International Conference on Data Engineering and Communication Technology*, pp. 319-331. Springer Singapore, 2017.

[3] J. R. Douceur, "The Sybil attack", *First International Workshop on Peer-to-Peer Systems* (IPTPS '02), 2002.

[4] C Karlof. And D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *AdHoc Networks*, Vol. 1, No. 2, pp. 299-302, 2003.

[5] A. Ajina, M. K. Nair, "Cross Layered Network Condition Aware Mobile-Wireless Multimedia Sensor Network Routing Protocol for Mission Critical Communication", *International Journal of Communication Networks and Information Security* (IJCNIS), Vol. 9, No. 1, 2017.

[6] J. Newsome, E. Shi, D Song. and A. Perrig, "The Sybil attack in sensor networks: analysis and defences", *International Symposium on Information Processing in Sensor Networks*, pp. 259–268, 2004.

[7] S. Zhong, L. Li, Y. G. Liu and Y. R. Yang, "Privacy-preserving location based services for mobile users in Wireless Networks", Technical Report YALEU/DCS/TR-1297, Yale Computer Science, 2004.

[8] M. Demirbas and Y. Song, "An RSSI-based scheme for Sybil attack detection in wireless sensor networks" *IEEE Computer Society International Symposium on World of Wireless, Mobile and Multimedia Networks*, pp. 570–574, 2006.

[9] S. Misra and S. Myneni, "On Identifying Power Control Performing Sybil Nodes in Wireless Sensor Networks Using RSSI*", IEEE Global Telecommunications Conference* (GLOBECOM), pp. 1-4, 2010.

[10] S. Chen, G. Yang, and S. Chen, "A Security Routing Mechanism against Sybil Attack for Wireless Sensor Networks", *International Conference on Communications and Mobile Computing*, 2010.

[11] A. Jangra, P. Swati, "Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)", *International Conference on Advances in ICT for Emerging Regions*, pp. 79-87, 2011.

[12] WANG X.-D., SUN Y.-Q. and MENG X.-X.: Cluster-based Defending Mechanism for Sybil Attacks in Wireless Sensor Network. *Computer Engineering*, Vol. 15, 2009.

[13] W. Shi, S. Liu, and Z. Zhang, "A Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network", *KSII Transactions on Internet & Information Systems*, Vol. 9, No. 9, pp. 3738-3749, 2015.

[14] M. Jamshidi, A. Hannani, M. Esnaashari, and M. R. Meybodi, "Defending Sybil Attack in Wireless Sensor Networks with the aid of Detecting Suspicious Arias in the Network", *20th Computer Soceity of Iran Annual Conference*, University of Mashhad, Mashhad, Iran, 2-4, 2015.

[15] K. F. Ssu, W. T. Wang, and W. C. Chang, "Detecting Sybil attacks in wireless Sensor Networks using neighboring information", *Computer Networks*, Vol. 53, No. 18, pp. 3042–3056, 2009.

[16] R. Rafeh, and M. Khodadadi, "Detecting Sybil Nodes in Wireless Sensor Networks Using Two-hop Messages", *Indian Journal of Science and Technology*, Vol. 7, No. 9, pp. 1359-1368, 2014.

[17] S. Ramachandran and V. Shanmugan, "Impact of Sybil and Wormhole Attacks in Location based Geographic Multicast Routing Protocol for Wireless Sensor Networks", *Journal of Computer Science*, Vol. 7, No. 7, pp. 973-979, 2011.

[18] R. Muraleedharan, X. Ye, and L.A. Osadciw, "Prediction of Sybil Attack on WSN Using Bayesian Network and Swarm Intelligence", *Wireless Sensing and Processing*, Orlando, FL, USA, 2008.

[19] S. Sharmila and G. Umamaheswari, "Detection of Sybil attack in mobile wireless sensor networks", *International journal of engineering science & advanced technology*, Vol. 2, pp. 256 – 262, 2012.

[20] S. Sharmilaa and G. Umamaheswari, "Node ID based detection of Sybil attack in mobile wireless sensor network", *International Journal of Electronics*, Vol. 100, No. 10, pp. 1441-1454, 2012.

[21] M. Jamshidi, E. Zangeneh, M. Esnaashari, and M. R. Meybodi, "A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks", *Computers & Electrical Engineering*, 64, pp. 220-232.

[22] S. Rupinder, J. Singh, and R Singh, "TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks", *International Journal of Computer Science and Network Security* (IJCSNS), Vol. 16, No. 11, 2016.

[23] U. S. Dhamodharan and R. Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", *The Scientific World Journal*, Vol. 1, No. 1, pp. 13-17, 2015.

[24] R. Amuthavalli and R. S. Bhuvaneswaran, "DETECTION AND PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK EMPLOYING RANDOM PASSWORD COMPARISON METHOD", *Journal of Theoretical & Applied Information Technology*, Vol. 67, No. 1, pp.236-246, 2014.

[25] S. Sinha, A. Paul, and S. Pal, "Use of Spline Curve in Sybil Attack Detection based on Received Signal Power-New Approach", *International Journal on Recent Trends in Engineering & Technology*, Vol. 11, No. 1, pp. 602-611, 2014.

[26] S. Panagiotis, E. Karapistoli, and A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information", *Expert Systems with Applications*, Vol. 42, No. 21, pp. 7560-7572, 2015.

[27] R.-H. Hu, X.-M. Dong, and D.-L. Wang, "Defense mechanism against node replication attacks and Sybil attacks in wireless sensor networks", *Acta Electronica Sinica*, Vol. 43, No. 4, pp. 744-752, 2015.

[28] J-SIM Simulator, https://sites.google.com/site/jsimofficial/, December 25, 2017.

[29] C. M. Yu, C. S. Lu, and S. Y. Kuo, "Mobile Sensor Network Resilient Against Node Replication Attacks", *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (SECON), 2008.