ORIGINAL RESEARCH PAPER
Pages: 205-219

The Evolutionary Game-Based Dynamics of Sybil Attack Prevention in WSN

A. Navaei Tourani[1], H. Haj Seyyed Javadi[2], H.R. Navidi[2], A. Sharifi[1]
1.Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
2.Department of Mathematics and Computer Science, Shahid University, Tehran, Iran
Azadehnaveii@gmail.com, h.s.javadi@shahed.ac.ir, Navidi@shahes.ac.ir, a.sharifi@srbiau.ac.ir
Corresponding author: h.s.javadi@shahed.ac.ir

DOI:10.22070/JCE.2023.17301.1235

Abstract- Today, wireless sensor networks are widely employed in various applications, including monitoring environments and tracking objects for military surveillance, industrial applications, and healthcare. Thus, the establishment of security in such networks is of great importance. One of the dangerous attacks against these networks is the Sybil attack. In this attack, a malicious node propagates multiple fake identities simultaneously, which affects routing protocols and many other operations like voting, reputation evaluation, and data aggregation. In this paper, we study the sensor node rate trust decision to defend against Sybil attacks in WSNs and its dynamics that play a key role in stabilizing the whole WSN using evolutionary game theory. We then propose and prove the theorems indicating that evolutionarily stable strategies can be attained under different parameter values, which supply the theoretical foundations to devise defiance against Sybil attacks in WSNs. Moreover, we can find out the conditions that will lead SNs to choose the strategy Healthy as their final behavior. In this manner, we can assure WSNs' security and stability by introducing a rate-trust mechanism to satisfy these conditions. And furthermore, the efficiency of algorithms in terms of true detection rate and false detection rate is evaluated through a series of experiments. Experiment results show that the proposed algorithm is able to detect 99.9% of Sybil nodes with a 0.005% false detection rate. Additionally, the proposed algorithm is compared with other algorithms in terms of true detection rate and false detection rate, which shows that the proposed algorithm performs satisfactorily.

Index Terms- Sybil attacks, Wireless Sensor Networks, Game theory, healthy strategy, Sybil strategy.

I. INTRODUCTION

Wireless sensor networks (WSNs) can be widely applied to a great many applications, such as monitoring environments and tracking objects for military surveillance, industrial applications, and healthcare [1] [2]. WSNs are highly distributive by nature and self-organised in functionality. A WSN

Manuscript received 15-March-2021 and revised 11-May-2021, *P-ISSN: 2322-4088*
Accepted on 13- June-2021 *E-ISSN:2322-3936*

incorporates numerous tiny sensor nodes in its network, thereby creating an environment that can sense and collect information about certain phenomena [3] [4]. They are routinely installed in unsupervised and even hostile areas. The wireless and resource-constrained nature of an SN makes it an ideal medium for attackers to perform any kind of malicious activity; therefore, achieving an adequate level of security is a difficult task [4] [5] .

Many security mechanisms have been proposed to address security concerns such as eavesdropping, message replay, and message fabrication. Nevertheless, although these tactics are effective against external network attacks, they do not work effectively when confronting internal attacks. This is due to the fact that SNs conducting internal assaults can obtain all required cryptographic keys and thus become lawful members of other networks. To guarantee secure key exchange and establish secure communication, designers must first ensure that all communicating nodes are trusted [1] [6].In a Sybil attack, the attacker either inserts a malicious node into the network or captures a legitimate node to reprogram and reintroduce it. By assuming these identities, the malicious node can fool legitimate nodes into believing they have a large number of neighbours. As a result, these malicious nodes cause additional traffic, destabilise the routing protocol, and impair network processes such as data aggregation, voting, reputation evaluation, and equitable resource allocation [3] [7] [8].

Regarding the article [6], a trust rate management system offers a hybrid of direct and indirect observation trust rate SNs based on present and past vector time. Issues such as network traffic and congestion were not considered in as well as our proposed model. Based on the network conditions and factors, the population of WSNs will be more inclined toward one of the two strategies, collaboration or sybil. Depending on the popularity of each strategy in the population, more SNs will follow it. Since the description of the trust rate management system is not the major topic of this paper, we do not review it closely in our proposed model [2] [9].

In this paper, on the basis of evolutionary game theory, SNs are considered individual players, and the entire population of WSNs is the population. A trust game between WSNs is set up because each SN can choose a different strategy [6]. Moreover, an incentive mechanism integrated into the game is also introduced to investigate the mechanism’s effect on stimulating an SN to choose the collaboration strategy. We then investigate evolutionarily stable strategies (ESSs) of the proposed game with the idea of replicator dynamics. Strategies that effectively promote the collaboration strategy in the population The rest of this paper is organised as follows: In Section 2, the related works are surveyed. In Section 3, the proposed WSNs' trust games are then depicted, and their ESSs are investigated with the idea of replicator dynamics. Section 4 describes the experiments to confirm the ESSs of the proposed WSNs trust game and the effects of the incentive mechanism. Finally, conclusions are presented in Section 5.

II. RELATED WORK

Douceur [10], introducing the Sybil attack, indicated that peer-to-peer networks are vulnerable to it. Karloff [11]argued that this assault might affect sensor network routing methods. They also created taxonomies for Sybil attacks in terms of identity construction, Sybil node communication, and simultaneity, which are referred to in the bulk of the studies. Additionally, methods for detecting Sybil nodes by radio resource testing, detecting Sybil nodes via random key redistribution, fighting against Sybil attacks using identity registration, and performing remote code verification or code attestation are provided. Chen et al [12] proposed using RRSI to discover Sybil nodes in WSNs using the LEACH routing protocol. In the Sybil attack model, in which a malicious node acts as a cluster head, an intrusion election system is activated when the number of cluster heads exceeds Copts. This mechanism is centralised and has problems in terms of scalability. Ssu et al [13]. demonstrated a distributive strategy for locating Sybil nodes that does not require hardware or signal strength information and instead relies on the number of neighbours.Misra and Myneni [14].proposed a strategy for identifying Sybil nodes based on increased RSSI, which prevents Sybil nodes from being disguised by varying power. Li et al [15]. Through a co-presence state diagram, each watchdog node delivers partial information. A selected watchdog node collects all the missing information and uses a detection criterion to identify the Sybil nodes. Almas et al [16]. presented a technique for identifying Sybil nodes in mobile WSNs that relies on watchdog nodes to monitor Hello packet exchanges between nodes. Through a co-presence state diagram, each watchdog node delivers partial information. Dhamodharan and Vayanaperumal [17]. suggested an algorithm for identifying Sybil nodes in WSNs using message authentication. This strategy utilises message authentication before establishing communication and transmitting messages. Without authorization from the base station, no SN can connect with other nodes in the network. Sinha et al [18]. suggested an algorithm to identify the Sybil attacks using the characteristics of the nodes' received signal strengths. Rafeh and Khodadad [19].suggested a distributed system for detecting Sybil nodes in WSNs based on two-hop message propagation. Nodes can identify the Sybil nodes by sending messages to each of the two-hop neighbours they share with the neighbour nodes. Additionally, Jamshidi et al [20]. suggested a fast, lightweight technique for identifying Sybil nodes in mobile WSNs. This method labels (bit labels) mobile nodes based on their movement characteristics and then finds the Sybil nodes according to those labels. Jamshidi et al [21]. suggested another approach for detecting Sybil assaults in mobile WSNs that employ active nodes. Tayyab khan et al [7]. proposes a dual trust-based multi-level Sybil (DTMS) attack detection approach in WSNs. The work engages a multi-level detection system grounded on the verification of the node's identity and location.a Also at each level, CM, CH, and BS, the trust value is calculated. The trust function of DTMS involves dynamic reward and penalty coefficient to ensure severity. The summary of the studied articles is presented in TableI.

Table I. Sybil attack detection algorithms.

Algorithm	Network type	Location information	Specific topology	Centralized	explanations
Chen et al [12].	Stationary	Yes	Yes	Yes	RSSI and clustering are used.
Ssu et al [13].	Stationary	Yes	No	No	Discovers common neighbor by utilizing nearby information.
Misra and Myneni [14].	Stationary	Yes	No	No	RSSI is used to find the position of nodes.
Almas et al [16].	Mobil	Yes	No	No	Watchdog nodes and movement data are used.
Dhamodharan and Vayanaperumal [17].	Stationary	Yes	No	No	"Compare and match-position verification technique" and "message authentication and passing" are combined.
Rafeh and Khodadadadi [19].	Stationary	Yes	No	No	sees adjacent data and sends out two-hop packets.
Jamshidi et al [20]	Mobil	Yes	No	No	assigns a bit label to nodes depending on their mobility via a distributed labelling method
Jamshidi et al [22]	Mobil	No	No	No	Uses observer nodes and information from nearby nodes.
Tayyab khan et al [7]	Stationary	Yes	No	No	The trust function of DTMS involves dynamic reward and penalty oefficient to ensure severity.

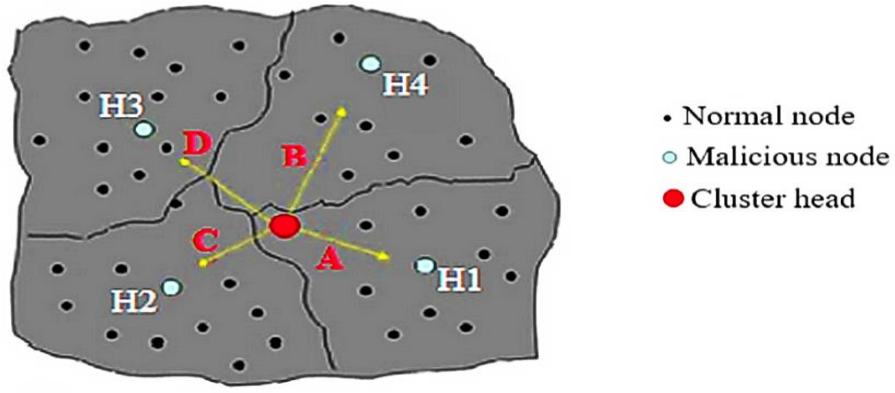

Fig. 1. An example of establishing a new Sybil attack model [23]

III. THE PROPOSED WSN SYBIL ATTACK GAME

A. Sybil attack model

In the Sybil Attack model proposal, a malicious node generates $1 < S \leq Copt$ Sybil IDs during each clustering phase (where Copt represents the number of clusters in the current phase) and then uses each created ID to join a new cluster. If Sybil nodes are linked to a large number of cluster heads, the sink node readily detects them and prevents malicious actions in the system. As result, a malicious node will not attempt to take over the cluster heads. Rather, it attempts to join each cluster member

using one of its Sybil identities. Therefore, the malicious node joins several or all clusters concurrently ،consequently, will have an impact on the operations and data of these clusters [23] [22].

Thus, the malicious node joins multiple or all clusters simultaneously. Consequently, a malicious node affects the operations and data of multiple clusters or all clusters. Fig I shows an example of such a Sybil attack. In this example, the malicious node with identities A, B, C, and D is a member of cluster heads H1, H4, H2, and H3, respectively. It should be noted that malicious nodes with different powers transmit joint messages to cluster heads. Further, when the cluster head is from the malicious node, a join message with more power is sent to the cluster head. In Section 4, an approach is also proposed to defend against it.

B. The proposed Algorithm to Defend against the Novel Sybil Attack Model in WSNs

Our topic of interest is to focus on the process of trust decisions made by sensor nodes to disclose the principle of trust evolving in WSNs. With the idea of evolutionary game theory, we consider sensor nodes as individuals and the WSNs as a population. We establish a trust game for sensor nodes according to the situation, i that various sensor nodes are able to select different strategies. Then, using replicator dynamics, we investigate evolutionarily stable game strategies to demonstrate the stability of WSNs.The conventions that are applied to define the WSN's trust rate game are presented as follows:

Convention 1: The WSN population depicted by p includes the SNs following both pure strategies (Healthy and Sybil).

Convention 2: The WSN's Sybil Attack game, which is symmetric, is formulated by a 3-tuple, where:

1. In the set of SN players, each player in the competition is represented by = [1, 2..., n].
2. In the equation, SN is a population vector that employs a pure strategy.
3. Table II defines what the payoff matrix is. Also, the applied parameters for payoffs are introduced in TableIII.

In general, a trust degree is used to assess the trust rating levels of SNs. Many authors proposed various trust rate degree computation strategies. In this paper, we do not take into account how to compute the trust rate level; however, we suppose that each sensor node already has a trust rate. In the Sybil Attack game, each sensor node may select the strategy "Healthy" or "Sybil." Selecting the strategy "Healthy" by a sensor node means that it will cooperate with its counterpart; on the other hand, selecting the strategy "Sybil" means noncooperation. According to Table II, different payoffs in various cases are discussed below.

Table II. Payoff matrix of the Sybil Attack game.

The strategy of the first player (α_1)	**The strategy of the second player** (α_2)	
	Healthy	**Sybil**
Healthy	$M_T + M_C - 2\beta$	$\mathrm{M_T} - \beta - \mathrm{L}$
Sybil	$M_T + M_C - \beta$	M_D

Table III. Effective parameters in defining the trust rate of the sensor node.

Parameter	**Meaning**
$\boldsymbol{M_T}$	Gain payoff by a sensor node selecting the strategy healthy
$\boldsymbol{M_s}$	Gain payoff by a sensor node selecting the strategy Sybil
$\boldsymbol{M_p}$	Cooperation gain of a sensor node due to its counterpart selecting the strategy healthy
L	Uncooperative loss of a sensor node due to its counterpart selecting the strategy Sybil
β	Cost caused by a sensor node transmitting its own or its opponents' sensed data.

Case 1: Two SNs have agreed to use the Healthy strategy: In this case, one of the two SNs cooperates with the other and supports its adversary in forwarding sensing data. As a result, their trust rate is increased, and they obtain a payoff equal to $M_T + M_C - 2\beta$

Case 2: One SN opts for the Healthy strategy, while its opponent opts for the Sybil strategy: The SN choosing the healthy strategy gains as a result of the improvement in its trust rate, which is received by forwarding its opponent's sensed data, and the incentive gain. Simultaneously, it must compensate for the cost caused by the computation and power consumption resulting from forwarding its opponent's sensed data. On the other hand, as the Sybil strategy is chosen by the opponent SN, no cooperation will occur between the two SNs. This will lead to the first SN's loss since its own sensed data cannot be transmitted to the expected SN. Therefore, they obtain a payoff equal to be $M_T + M_C - \beta$

Case 3: One SN opts for the Sybil strategy, while its opponent opts for the Healthy strategy: If the SN chooses the Sybil strategy, it will not need to forward its opponent's sensed data. Therefore, it will receive, and since there will be no need to consume its power, the SN's lifetime will be extended. It will also receive it, as the opponent has chosen the collaboration strategy. Simultaneously, it must compensate for a cost in order to transmit its own sensed data with success. Therefore, its entire payoff will $\mathrm{M_T} - \beta - \mathrm{L}$

Case 4: Both SNs choose Sybil's strategy: No cooperation is seen between the players in this case. As explained above, neither of them receives a payoff, and they obtain a payoff equal toM_D

C. Evolutionarily stable strategies of the Sybil attack detection Game

There are totally two strategies in the trust game, so, let θ(t)={θ,θ-1} be the mixed-strategy at time t in the population P, where β denotes the rate of sensor nodes selecting strategy Sl (Healthy), then the rate of sensor nodes selecting strategy S2 (Sybil) is β-1. According to evolutionary game theory [6], the expected payoff of sensor nodes selecting the strategy Trust is.

$$u(\alpha_1, \theta(t)) = \beta(M_T + M_C - 2\beta) + (1 - \beta)(M_T - \beta - L) \quad (1)$$

And the expected payoff of SNs choosing the Sybil strategy is computed using Eq. 7.

$$u(\alpha_1, \theta(t)) = \beta(M_T + M_C - 2\beta) + (1 - \beta)(M_T - \beta - L) \quad (2)$$

The average payoff of the whole population P is

$$\bar{u}(\theta(t), \theta(t)) = \theta u(s_1, \theta(t)) + (1 - \theta)(s_2, \theta(t)) \quad (3)$$

The replicator dynamics equation of trust evolving in WSNs, therefore, is calculated according to Eq. 4.

$$F(\theta) = \dot{\theta} = \theta \left(u(s_1, \theta(t)) - \bar{u}(\theta(t), \theta(t))\right) =$$

$$\theta(1 - \theta)[\theta(M_c + M_D - \beta) + (1 - \theta)(M_T + M_D - \beta - \mathrm{L})] \quad (4)$$

Let F (B) = 0, then Eq. (4) has three stable states at most that are

$$\theta_1^* = 0, \quad (5)$$

$$\theta_2^* = 1, \quad (6)$$

$$\theta_3^* = \frac{(M_D + \beta + L - M_T)}{L} \quad (7)$$

According to characteristics of evolutionarily stable strategy, a stable state must be immune to a small disturbance, which is actually accordant to the requirements of the stable theorem of differential equation. That is, must be satisfied when F^' (θ^*)<0is a stables state.

Theorem1.When $M_T - M_D - \beta > 0$, $M_D + \beta + \mathrm{L} - M_T > 0$, and $2M_T + 2M_d - 2\beta - \mathrm{L} > 0$ and $2M_T + 2M_D - 2\beta - \mathrm{L} > 0$, $\theta_1^* = 0$ *and* $\theta_2^* = 1$ are evolutionarily stable strategies of the Sybil Attack game for sensor nodes, which satisfy $\rho(\theta_1^* = 0) < \rho(\theta_2^* = 1)$ Where $\rho(\theta_1^* = 0)$ and $\rho(\theta_2^* = 1)$ indicate denote the probability of sensor nodes selecting the strategy Sybil and that of ones selecting the strategy Healthy, respectively.

Proof: Calculating the derivative of Eq. (4), the following is attained:

$$\acute{F}(\theta) = -3L\theta^2 + (2M_D + 2\beta + 4L - 2M_T)\theta + M_T + M_D - \beta - L \quad (8)$$

Let $\theta = 0$ and $\theta = 1$, respectively, we get

$$\acute{F}(0) = M_T - M_D - \beta - \mathrm{L} < 0 \quad (9)$$

$$\acute{F}(1) = M_D + \beta - M_T < 0 \quad (10)$$

Since

$$2M_T - 2M_D - 2\beta - \mathrm{L} > 0 \quad (11)$$

We get

$$M_T - M_D - \beta > M_D - \beta + L - M_T \quad (12)$$

So, we get

$$0 < \frac{M_D + \beta + L - M_T}{\mathrm{L}} = \frac{M_D + \mathrm{L} + \beta - M_T}{M_T - M_D - \beta + M_D + \mathrm{L} + \beta - M_T} < \frac{M_D + \mathrm{L} + \beta - M_T}{2(M_D + \mathrm{L} + \beta - M_T)} = \frac{1}{2} \quad (13)$$

According to equations (9), (10) and (13), both$\theta_1^* = 0$ and $\theta_2^* = 1$ are evolutionarily stable

strategies. What is more, according to Eq. (13), the probability of sensor nodes selecting the strategy Sybil is less than that of ones selecting the strategy Trust, i.e., $(\theta_1^* = 0) < \rho(\theta_2^* = 1)$.

Theorem 2. When $M_T - M_D - \beta > 0$, $M_D + \beta + L - M_T > 0$, and $2M_T + 2M_d - 2\beta - L < 0$, both $\theta_1^* = 0$ and $\theta_2^* = 1$ are evolutionarily stable strategies of the Sybil Attack game for sensor nodes, which satisfy $\rho(\theta_1^* = 0) > \rho(\theta_2^* = 1)$.

Proof Similar to the proof of Theorem 1, we can get

$$\acute{F}(0) = M_T - M_D - \beta - \mathrm{L} < 0 \tag{14}$$

$$\acute{F}(1) = M_D + \beta - M_T < 0 \tag{15}$$

$$\frac{1}{2} < M_D + \beta + L - M_T \backslash L < 1, \tag{16}$$

According to equations (14), (15), and (16), both $\theta_1^* = 0$ and $\theta_2^* = 1$ are evolutionarily stable strategies. What is more, according to Eq. (16), the probability of sensor nodes selecting the strategy Sybil is more than that of ones selecting the strategy Healthy, i.e., $\rho(\theta_1^* = 0) > \rho(\theta_2^* = 1)$.

Theorem 3. When $M_T - M_D - \beta < 0$, both $\theta_1^* = 0$ is the only evolutionarily stable strategy of the Sybil Attack game for sensor nodes.

Proof Similar, we can get.

$$\acute{F}(0) = M_T - M_D - \beta - \mathrm{L} < 0. \tag{16}$$

$$\acute{F}(1) = M_D + \beta - M_T > 0 \tag{17}$$

According to equations (17) and (18), $\theta_1^* = 0$, therefore, is the evolutionarily stable strategy.

Theorem 4. When $M_T - M_D - \beta - L > 0$, both $\theta_2^* = 1$ is the only evolutionarily stable strategy of the Sybil Attack game for sensor nodes.

Proof Similar, we can get.

$$\acute{F}(0) = M_T - M_D - \beta - \mathrm{L} < 0, \tag{18}$$

$$\acute{F}(1) = M_D + \beta - M_T > 0 \tag{19}$$

According to theorems 1-4, a trust management system must satisfy conditions of Theorem 1 or 4 that will promote sensor nodes to select the strategy Healthy, thus the security and stability Of WSNs can be guaranteed. Apparently, we must avoid satisfying the conditions of Theorem 2 or 3 when designing a true management system. Otherwise, the probability of sensor nodes selecting the strategy Sybil is larger than that of ones selecting the strategy Healthy, all sensor nodes ultimately select the strategy Sybil as their stable state. This situation that we do not expect to see will make WSNs unstable.

Table IV. Simulation Parameters

Parameter	Level

Area	500m x 500m
Propagation Model	Two-ray ground reflection
Number of sensor nodes(N)	100
Number of sensor nodes (M)	1
Number of sensor nodes(S)	7
MAC	802.11
Omnidirectional	Omnidirectional
Simulation Time	10 s
Placement	Random
clusters Cluster	4
Nodes in Cluster	C_{opt}
Node Initial Energy	90J
Equal energy (startup)	Yes
Packet size	500
Pause time	3secs

III. SIMULATION AND EXPERIMENT RESULTS

The proposed algorithm is simulated using Mat lab r2010a software, and we verify evolutionarily stable strategies of the Sybil Attack game under different parameter values in table IV of and.; the corresponding changeable trends of curves are illustrated in Fig. 1 and 3, which are respectively related to the four cases above.

a. Simulation Assumptions

- As illustrated in FigII, the N sensor nodes are randomly spread throughout a 500 × 500-meter region.
- Throughout the network, all sensor nodes are homogenous and have unique ID numbers.
- The network is divided into C_opt clusters and runs on the LEACH routing protocol.
- Sensor nodes with M nodes are referred to as (Sybil) Sybil nodes.
- Sybil exposes numerous false IDs for each Sensor node (S).
- The network's sink node/base station is permanently installed in the network's core.

To ensure the validity of the simulation results, each experiment is repeated until the end of the Sensor nodes network life.

Evaluations of the implementation results of the proposed algorithm are examined in the following two sections.

- Investigation and evaluation of the effects of incentive mechanism and the ESSs of our WSNs trust rate game.
- Evaluating efficiency of the proposed algorithms with the evolutionary game theory approach with another algorithm.

In the first group, after initializing the parameter values to satisfy the conditions of Theorems 4-1,

respectively, we observe the changeable trends of trust evolution curves of Sensor node in WSNs. In the Second group, the experiment was performed to evaluate the performance of the proposed algorithm and also the results were compared with the proposed algorithms based on the following three performance criteria [12] [13] [14] [16] [17] [19] [20] [22] [7].

b. Evaluate the strategy and behavior process

In Fig. 2, the parameter values corresponding to the curve x satisfy the conditions of Theorem l. When the initial value of Eq.(4) is 0.401 that means 40.1% of sensor nodes have selected the strategy Healthy in the beginning, we can find that sensor nodes adjust their strategies continuously and, after about 38 times of playing the game, the rate of sensor nodes selecting the strategy Healthy will be stable at $\theta_2^* = 1$. When the initial value of Eq. (4) is 0.399 that means 39.9% of sensor nodes have selected the strategy Trust in the beginning, the rate of sensor nodes selecting the strategy Healthy, after about 44 times of playing the game, will be stable at $\theta_1^* = 0$ These results reflect that both $(\theta_1^* = 0)and(\theta_2^* = 1)$.are evolutionarily stable strategies of the Sybil Attack game for sensor nodes, and that$\rho(\theta_1^* = 0) < \rho(\theta_2^* = 1)$. Is satisfied under the conditions of Theorem l.

In Fig. 2, the parameter values corresponding to the curve x satisfy the conditions of Theorem 2. When the initial value of Eq. (4) is 0.801 that means 80.l% sensor nodes have selected the strategy Healthy in the beginning, the rate of sensor nodes selecting the strategy Healthy, after about 30 times of playing the game, will be stable at $(\theta_2^* = 1)$. When the initial value of Eq. (4) is 0.799 that means 79.9% of sensor nodes have selected the strategy Healthy in the beginning, the rate of sensor nodes selecting the strategy Healthy, after about 56 times of playing the game, will be stable at$(\theta_1^* = 0)$.

These results reflect that both$\theta_1^* = 0$ and $\theta_2^* = 1\, are$ evolutionarily stable strategies of the Sybil Attack game for sensor nodes, and that $\rho(\theta_1^* = 0) > \rho(\theta_2^* = 1)$ is satisfied under the conditions of Theorem 2.

In Fig. 3, the parameter values corresponding to the curve x satisfy the condition of Theorem 3. Even if 99.9% of sensor nodes have selected the strategy Healthy in the beginning, we can find that, after about 58 times of playing the game, the rate of sensor nodes selecting the strategy Healthy will be stable at $\theta_1^* = 0$ in the end. This result reflects that $\theta_1^* = 0$ is the evolutionarily stable strategy of the trust game for sensor nodes under the condition of Theorem 3.

In Fig. 2, the parameter values corresponding to the curve x satisfy Y the condition of Theorem 4. If only 0.1% of sensor nodes selected the strategy Healthy in the beginning, we can find that, after about 53 times of playing the game, the rate of sensor nodes selecting the strategy Healthy will be stable at $\theta_2^* = 1$ at the end. This result reflects that $\theta_2^* = 1$ is the evolutionarily stable strategy of the Sybil

Table V. Payoff matrix of the Sybil Attack game.

Parameter	parameter			
	M_T	M_D	β	L
$Group1$	14	3	8	5
$Group2$	12	3	8	5
$Group3$	12	3	8	5
$Group4$	17	3	8	5

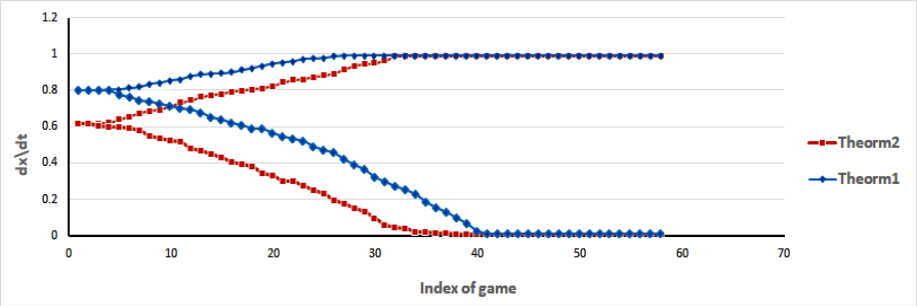

Fig. 2. Curves of Healthy evolving of sensor nodes (I)

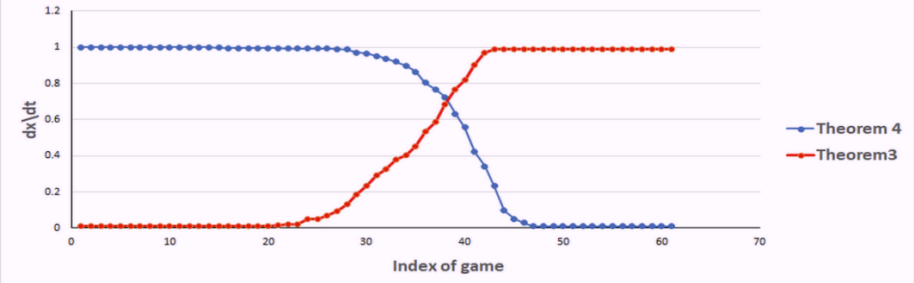

Fig. 3. Curves of Healthy evolving of sensor nodes (2)

attack game for sensor nodes under the condition of Theorem 4.

C.Comparing the suggested algorithm efficiency to that of another algorithm

A variety of tests are performed to evaluate its performance. The acquired results were also compared to the suggested algorithms in [16] [17] [19] [20] [22] [7].Three performance indicators were considered

- True Detection Rate (TDR) is the percentage of Sybil nodes which are detected by a security algorithm.
- False Detection Rate (FDR) is the percentage of normal nodes erroneously marked as Sybil nodes by a security algorithm.
- TDR/FDR Average is used to average the acquired results.

Fig 5 (a) shows that adding malicious (Sybil) sensor nodes to clusters boosts the actual detection rate

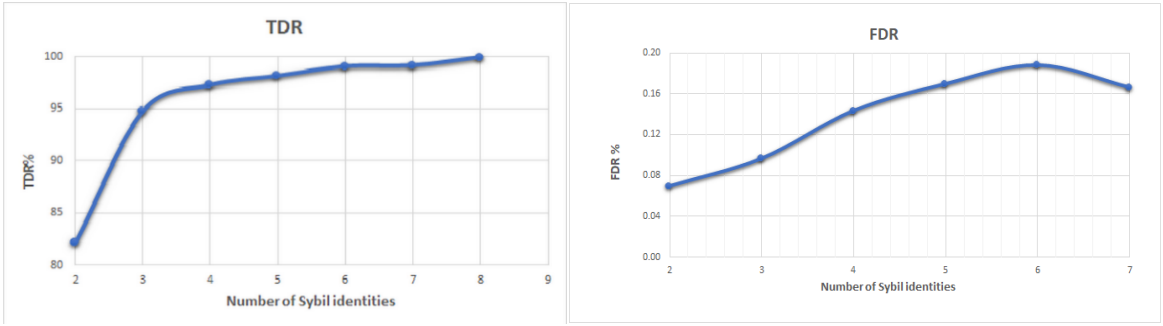

Fig. 4 The suggested algorithm's effect on the total number of nodes (N). (a) On the correct detection rate and (b) the erroneous detection rate.

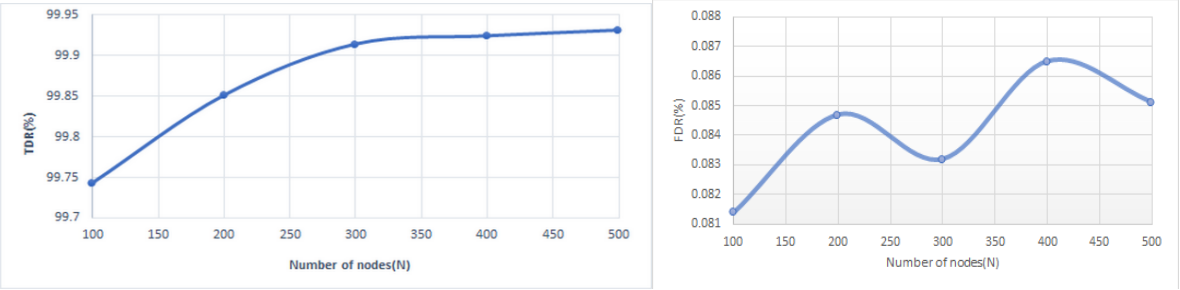

Fig. 5. Effect of the number of total nodes (N) of the proposed algorithm. (a) On true detection rate (b) on false detection rate.

(TDR) of the proposed approach for the following two reasons:

- If the malicious sensor node joins several clusters at the same time, the detection rate of malicious sensor nodes increases.
- If the malicious sensor node joins clusters with fewer fake identities, the suggested algorithm's likelihood of detecting them lowers.

Furthermore, as shown in Fig. 4 (b), the suggested algorithm's FDR for S = 2 and S = 3 is 0.047 per cent and 0.087 %, respectively, while for S > 3 it is around 0.113 %. As seen in Scenario 1, certain lawful nodes may be mistakenly identified as Sybil nodes throughout each run of the detection method. As a result, increasing S (malicious node joins more clusters) raises the number of FDR.

In Fig 5 (a), the parameters are changed to S = 5, M = 1, Copt = 7, and N changes from 100 to 500 (with a step of 100), and the influence on the suggested algorithm's performance is assessed. The True Detection Rate (TDR) is shown in Fig 4 (a), the False Detection Rate (FDR) is shown in Fig 4 (b).

In this Experiment, parameters are adjusted as S = 5, M = 1, Copt = 7, and $T_{min} = 2$ and N vary from 100 to 500 (with step 100) and its impact on the performance of the proposed algorithm is evaluated. Fig. 5 (a) shows True Detection Rate (TDR), and Fig. 5 (b) shows False Detection Rate (FDR). Experiment results show that increasing the number of nodes increases all TDR, FDR and communication overhead of the proposed algorithm.

Table VI. Comparison of the performance of the proposed algorithm in terms of TDR and FDR rates with other existing algorithms.

Algorithm	Average TDR (%)	Average FDR (%)
Chen et al [12].	92%	**2%**
Ssu et al [13].	99%	**5%**
Misra et al [14].	98%	**6%**
Almas et al [16].	98%	**1%**
Dhamodharan et al [17].	80%	**1%**
Rafeh et al [19].	98%	**3%**
Jamshidi et al [20].	94%	**2%**
Tayyab khan et al [7].	98.80%	**0.08%**
Proposed algorithm	99.90%	**0.05%**

In the last Experiment, the proposed algorithm's performance is compared to that of other existing algorithms in terms of True Detection Rate (TDR) and False Detection Rate (FDR) [12] [13] [14] [16] [17] [19] [20] [22] [7].

Two types of algorithms are represented in this collection:

1. The suggested approach, as well as the algorithms in [12] [13] [14], are suitable for stationary WSNs.
2. Algorithms suitable for mobile WSNs as described in [16] [17] [19] [20] [22] [7].

The attack model and the proposed attack detection are different from other algorithms, the performance of the proposed algorithm cannot be compared with other algorithms in terms of TDR and FDR. But this comparison can the average efficiency algorithms with each other. Thus, here presents a comparative analysis of algorithms (average TDR and FDR) of the proposed algorithm by other algorithms are compared. Table 10 shows the comparison result. As can be seen in the results, the proposed algorithm with an average TDR of 99.9% outperforms other algorithms. Also, the average FDR of the proposed algorithm is 0.05% which indicates its performance is desirable.

IV. CONCLUSION

Trust relations among sensor nodes can help build their confidence and reduce the risk of cooperation. The Sybil Attack game for sensor nodes that we have built can reflect sensor nodes' utilities when deciding whether to use the "Healthy or Sybil" strategy we have achieved the replicator dynamics equation of trust. Evolving, which constructs a method to explore various evolutionarily stable strategies under different parameter values. These evolutionarily stable strategies have indicated how the dynamic system of trust evolving in WSNs ultimately reaches its stable point after the participating sensor nodes have continuously adjusted their strategies, which have also laid the foundation to design a trust management system. The results from experiments under different parameter values, evolutionarily stable strategies of the trust game for sensor nodes According to with these evolutionarily stable strategies, we must, when designing a trust management system, satisfying the conditions that will make.

REFERENCES

[1] K. Muthukumaran, K. Chitra, and C. Selvakumar, "An energy efficient clustering scheme using multilevel routing for wireless sensor network," *Computers & Electrical Engineering*, vol. 69, pp. 642-652, July 2018 .

[2] D.E. Ganesh, "Analysis of wireless sensor networks through secure routing protocols using directed diffusion methods," *International Journal of Wireless Network Security*, vol. 7, no. 1, pp. 28-35, Aug. 2022.

[3] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of computer and system sciences*, vol. 80, no. 3, pp. 644-653, May 2014.

[4] R. Sinde, F. Begum, K. Njau, and S. Kaijage, "Refining network lifetime of wireless sensor network using energy-efficient clustering and DRL-based sleep scheduling," *Sensors*, vol. 20, no. 5, p. 1540, Aug. 2020.

[5] N. Masaeli, H. Haj Seyyed Javadi, and S.H. Erfani, "Survey of Effective of Combinatorial Design Schemes in Wireless Sensor Networks Security," *Journal of Communication Engineering*, vol. 9, no. 2, pp. 271-282, Apr. 2020.

[6] L. Yi, W. Fang, W. Zhang, W. Gao, and B. Li, "Game-based trust in complex networks: Past, Present, and Future," *Complexity*, vol. 2021, pp. 1-7, Aug. 2021.

[7] T. Khan and K. Singh, "DTMS: A Dual Trust-based Multi-level Sybil Attack Detection Approach in WSNs," DOI:10.21203/rs.3.rs-2566539/v1, March 2023.

[8] M. Sadeghizadeh and O.R. Marouzi, "Securing cluster-heads in wireless sensor networks by a hybrid intrusion detection system based on data mining," *Journal of Communication Engineering*, vol. 8, 1, pp. 1-19, Mar. 2019.

[9] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," *Security and Communication Networks*, vol. 8, no. 9, pp. 1812-1827, June 2015.

[10] J.R. Douceur, "The Sybil attack," *First international workshop on peer-to-peer systems (IPTPS '02).,* pp. 251-260, 2002.

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293-315, Sept. 2003.

[12] S. Chen, G. Yang, S. Chen, "A security routing mechanism against sybil attack for wireless sensor networks," *In 2010 International Conference on Communications and Mobile Computing,*, pp. 142-146, April 2010,

[13] 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, Aug. 2009.

[14] S. Misra and S. Myneni, "On identifying power control performing sybil nodes in wireless sensor networks using RSSI," *In 2010 IEEE Global Telecommunications Conference GLOBECOM 2*, pp. 1-5, Dec. 2010.

[15] F. Li, P. Mittal, M. Caesar, and N. Borisov, "Sybil control: Practical Sybil defense with computational puzzles," *In Seventh ACM workshop on Scalable trusted computing*, p. 67–68, July2012 .

[16] S.R. Almas, K. Faez, F. Eshghi, and M. Kelarestaghi, "A new lightweight watchdog-based algorithm for detecting Sybil nodes in mobile WSNs," *Future Internet*, vol. 10, no.1, p. 1–17, 2017.

[17] U.S.R.K. Dhamodharan and R. Vayanaperumal, "Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method," *The Scientifc World Journal*, vol.2015, Article ID 841267, May 2015.

[18] 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, p. 602, Apr. 2014.

[19] R. Rafeh and M. Khodadadi, "Detecting Sybil nodes in wireless sensor networks using twohop messages," *Indian Journal of Science and Technology*, vol. 7, no.9, pp. 1359–1368, Aug. 2014.

[20] M. Jamshidi, M. Ranjbari, M. Esnaashari, N.N. Qader, and M.R. Meybodi, "Sybil node detection in mobile wireless sensor networks using observer nodes," *International Journal on Informatics Visualization,* vol. 2, no. 3, pp. 159–165, June 2018.

[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,* vol. 64, p. 220–232, Mar. 2017.

[22] G. Han, J. Jiang, L. Shu, J. Niu, and H.C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey," *Journal of Computer and System Sciences,* vol. 80, no. 3, pp. 602-617, Apr. 2014.

[23] M. Jamshidi, E. Zangeneh, M. Esnaashari, A.M. Darwesh, and M.R. Meybodi, "A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it," *Wireless Personal Communications,* vol. 105, pp. 145-17, May 2019.