ISSN 2515-8260 Volume 07, Issue 09, 2020

PRIVACY CONCERNED ANONYMOUS AUTHENTICATION METHOD FOR SYBIL ATTACK DETECTION IN WSN

L.Sheeba, *Assistant Professor, PSGR Krishnammal college for Women, Coimbatore.*
Dr.V.S.Meenakshi, *Research Supervisor, Chikkaana Government Arts College, Trippur*

ABSTRACT

Sybil attack is the most threatened issues found in the network which will cause consumption of more network spaces. Preventing the Sybil attack is difficult task where every fake identity generated by the attacker will looks like genuine id to the other nodes. In our previous work Sybil attack detection is performed through presenting an approach named Latency and Power aware Reliable Intrusion Detection System (LP-RIDS). However, this methodology failed in preventing Sybil attack occurrence which is focused in this work. In this work, Sybil attack prevention is ensured by introducing Privacy concerned Anonymous Authentication Method (PAAM). In this work, secondary cluster head selection is accomplished through Hybrid genetic with ACO algorithm. Here the secondary cluster head selection is done with the concern of higher energy value. The node that have energy lesser than threshold will not be considered for the Sybil node attack detection. And then anonymous authentication is performed to detect the Sybil attack. This is done by initializing the registration phase where all cluster members will share their temporal identity with the cluster head. Here temporal identity is generated randomly by each cluster member which is not possible to guess by other nodes. By using this temporal identity cluster head will generate the secret key which will be divided into two shares. Here first share will be given to the corresponding cluster member and second share will be given to the secondary cluster head. Thus no node can identify the privacy information of other users. This secret information will be utilized for the authentication process. Secondary cluster head will verify the cluster members at the time of data communication with the help of first share of secret key. This research method avoids the Sybil attack presence accurately. NS2 is greatly utilized in this research for validating the proposed techniques which offers better result when compared with prevailing work.

The overall implementation of the research work is done in the NS2 from which it is proved that the proposed techniques tends to provide better outcome than existing work.

Keywords: Intrusion detection, Sybil attack, secondary server, temporal identity, secret key share

I. INTRODUCTION

Wireless Sensor Network is greatly necessitated in various applications such as environmental monitoring, target tracking, health monitoring, and several maintenance operations [1]. Recent research work also demands two key activities namely Implementation and topology creation. Security is the key factor in wireless sensor network usage in variety of applications [2]. However, malicious attacks prevention and detection might be high or low in wireless sensor network [3]. Several attacks such as wormholes [4], sinkhole [5], Sybil [6], sleep [7], and selective forward attacks [8] exist so far in Wireless

Sensor Network. Their own infrastructure possessing portable devices deployed in different trade services in decentralized and scalable techniques are recognized by various researchers.

Synchronization capability by the devices do not use internet for multiuser applications at certain time. Precise location are obtained in the algorithm by this ability for accuracy enhancement. In case of Sybil attacker, wrong ID or duplicate ID of the users is shown who are aware of wireless sensor network nodes [9]. Alien nodes might occur in disguise in many identities and turn as original nodes in modern network background. Typically no common master node exists in social and defence network for monitoring communication amid network nodes intense.

Peer-to-peer network investigations reveals that these networks exhibits network logical functionalities or virtual networks coventry existence, i.e. networks built on other networks top as in internet [10]. Logical ID for structuring and forming networks tends to be the framework for network node addresses. Wireless sensor network nodes are not in static infrastructure, which might be single-hop, multi-hop communication, base station, gateways, and access points [11]. Mostly, smaller infrastructure may perhaps be non-infrastructure networks are comprised in Wireless Sensor Network.

Adhoc is chiefly meant for establishing for a distinct purpose and it is employed for tracking, function approximation and edge detection, monitoring environment, and security domain in the homeland. Wireless sensor network application is almost same as military force, monitoring restriction absence on infrastructure along with intermediate hop nodes. Different forms of Sybil attack exists namely Direct Communication, Indirect Communication, Fabricated Identities, Stolen Identities, Simultaneous and Non Simultaneous [12]. There are various sensor nodes limitations such as energy, lightweight solutions to secure against Sybil attack has to be investigated.

This research mainly focuses on Sybil attack prevention, which is implemented by adapting more recent techniques in the environment. This is done by introducing the various research methods which guarantees the accurate and effective prevention of Sybil attack occurrences.

II. RELATED WORKS

Amuthavalli et al [13] prevented Sybil attack by suggesting Random Password Comparison (RPC) technique which facilitates in node position controlling as well deployment. In addition, routing table creation is done in which every node's id information, time and password storage is done using algorithm along with identification of intermediate nodes amid source and destination is accomplished. Comparison of intermediate node's information with RPC database is performed. Normal node is recognized whenever information matches with node, else it reflected as Sybil node.

The authors in [14] suggested a methodology termed Relate and Identity Tactic (RAI) and Location Verification Technique (LVT) for preventing Sybil attack. Every system receives a key value in dynamic manner through BS in RAI whenever systems start interconnecting and sharing data. Sybil node is recognized when key matching does not happen with key agreed by BS. Also, Sybil system recognition is accomplished through nodes location verification in LVT.

In [15] established a Rule based Anomaly Detection System (RADS) for monitoring and identifying Sybil attacks in large scale WSN. It mainly relies on Ultra Wide Band (UWB) ranging based detection algorithm. Also it does not necessitate cooperation or information sharing amid sensor nodes. The operation of every node is done as an independent Anomaly based detection system (ADS) and mainly meant for detecting attacks only for it.

In [16], differentiation of legitimate nodes and Sybil nodes is recognized by suggesting an approach utilizing Received Signal Strength (RSS). Sybil identities are greatly accomplished deprived of utilizing third party. Transmissions signal strength are captured as well as stored by sensor network nodes sent through neighboring nodes. Threshold value refers to smallest readable RSS value. When new node entering into network happens, whenever node RSS is higher than threshold which means abnormal entry into neighborhood.

The authors in [17] suggested a RFID based system for Sybil attack prevention in Military Wireless Sensor Networks (MWSNs) in which two sort of authentication techniques are deployed. In first approach, RFID tags embedding are done for authentication and certification in soldiers. The second approach utilizes certificates through soldiers for authenticating them to their neighbors. Whenever two valid certificates are used by soldiers at same time, Sybil attack is identified through groups of soldier's leaders.

In [18] suggested Geographical and Energy Aware Routing (GEAR) protocol for packet routing toward target region by utilizing energy aware neighbor selection. Packet forwarding to nearest neighbor to destination is done when there occurs at least one closer neighbor to destination. A next hop is picked by GEAR minimizing cost value whenever all nodes are distant away. Forwarding decisions are done on the basis of local knowledge.

The author in [19] introduced Geographic Adaptive Fidelity (GAF) protocol which is an energy aware location-based routing algorithm and where complete area fragmenting is done into several square grids. GPS indicated location is exploited by node for associating itself with a point in virtual grid which adopts virtual grid data delivery model and every zone node acts as master. Also for definite time, it stays awaken which is responsible for monitoring and reporting data to sink.

In [20] suggested Greedy Perimeter Stateless Routing (GPSR) protocol which utilizes two phases for message forwarding, greedy forwarding and face routing. In case of greedy forwarding, packet forwarding to node closest to destination is done by every node. Greedy forwarding halting happens whenever closest node is identified. This dead end is known as local minima, local maxima, hole or void. GPSR entering into face routing or perimeter forwarding mode happens if message attains local minima.

III. PRIVACY CONCERNED ANONYMOUS AUTHENTICATION

In this work, secondary cluster head selection is accomplished through Hybrid genetic with ACO algorithm. Here the secondary cluster head selection is done with the concern of higher energy value. The node that have energy lesser than threshold will not be considered for the Sybil node attack detection. And then anonymous authentication is performed to detect the Sybil attack. This is done by initializing the registration phase where all cluster members will share their temporal identity with the cluster head. Here temporal identity is generated randomly by each cluster member which is not possible to guess by other nodes. By using this temporal identity cluster head will generate the secret key which will be divided into two shares. Here first share will be given to the corresponding cluster member and second share will be given to the secondary cluster head. Thus no node can identify the

privacy information of other users. This secret information will be utilized for the authentication process. Secondary cluster head will verify the cluster members at the time of data communication with the help of first share of secret key.

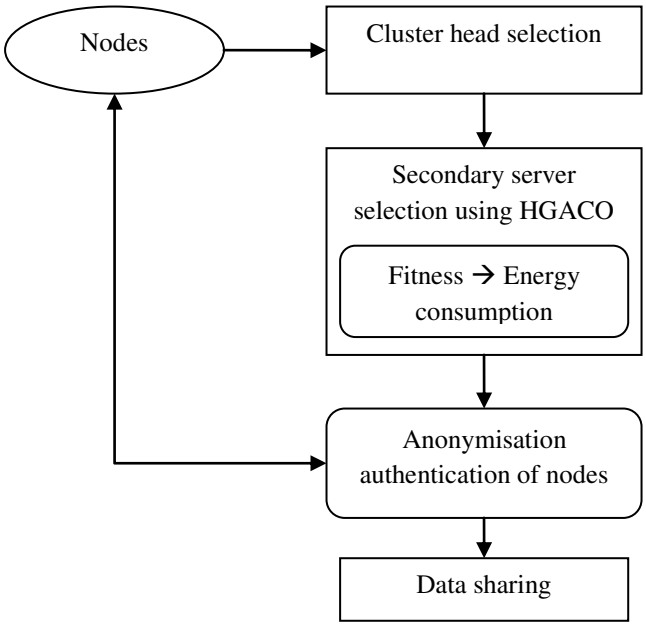


Figure 1. Overall flow of proposed method

3.1. NETWORK FORMATION

This research utilizes N numbers of nodes arbitrarily in network through administrator control. In addition, deployed nodes are finely configured, energy efficient, and promising in network. In the course of node creation, a $HELLO$ message is received by every node from BS with a timestamp message representing network node creation time (birth time). The Complete node corresponds to BS with a RES message with ID, timestamp, and location. Then this information storing is done in a $iNODEINFO\ table$ under network administrator control. The entire network model representation is specified as

$$G = \{(N1, N2, \ldots, Ni, \ldots, Nm), BS, \text{Admin}\}$$

Where, m is number of nodes in network.

Each node deployment is performed in network as Location (Ni) = (rand (x), rand (y)), where X, Y is any location inside network area. A HELLO packet is directed by BS to newly created nodes in network is `23454as follows

$$\mathrm{BS}(\mathrm{Msg}, \tau) \sum_{i=1}^{m} \mathrm{N_i}$$

Where N1, N2,...,Ni,...,Nm ➔ nodes

RES packet is sent to BS in network every node which is represented as Ni RES BS, in which HELLO and RES packet encompasses node ID and timestamp. HELLO = (Ni) and RES = (ID(Ni), $\tau(Ni)$), where Ni signifies ith node, $\tau(Ni)$ indicates ith node timestamp ,

ID(Ni) signifies ith node identity. The parameters such as ID and τ are utilized for node verification for checking Sybil node.

A node S necessitates for data transmission to node D in network G. Hence, route discovery is required from S to D by an N-hop intermediate node. Network size is mainly relied on number of intermediate nodes. AODV protocol is greatly utilized in routing mechanism. There is temporary storage of current information about the intermediate nodes (ID, timestamp) in routing table called as $iROUTING\ table$ throughout this process. Duration amid route discovery and data transmission in discovered route is considerably small. Despite the fact of data transmission, comparison of $iROUTING\ table$ data entries is done with entries existing in $iNODEINFO\ table$, aids in classifying duplicate nodes with id, timestamp, and the location.

3.2. SECONDARY SERVER SELECTION

In this work, secondary selection is carried out to reduce the burden involved in the sink node. If there is any attack present in the transmitted data which would affect the performance of the sink node directly. That will also cause performance degradation in other data transmission process. This can be avoided by separating the authentication process from the sink node. For this purpose here secondary server selection is carried in which authentication will be performed. In case of secondary server failure we can easily choose another node as secondary server, thus the performance cannot be compromised. Here nodes with higher energy value are preferred as secondary server. Optimal selection is ensured by introducing the method namely hybrid GA with ACO algorithm. The overall explanation of this method is specified in ensuing sub sections.

3.2.1. FITNESS CALCULATION

In wireless sensor network energy consumption is a major factor. Because when a node runs out of battery, it becomes a major problem in network. A dead node will affect entire communication. So the energy consumed by the network to detect a Sybil node is calculated. Equations (1) and (2) show the energy for cluster head and a node respectively.

$$E_N(ij) = bV_{sup}I_{sense}T_{sense} + bV_{sup}(I_{write}T_{write} + I_{read}T_{read}) + bE_{elec} + Bd_{ij}^{n}E_{amp} + T_AV_{sup}[C_NI_A + (1 - C_N)I_s]$$

$$\begin{aligned} ECH(j) = {} & h_3 bV_{sup}I_{sense}T_{sense} + h_4V_{sup}(I_{write}T_{write} + I_{read}T_{read}) + h_1b_1N_{CYC}C_{avg}V_{sup}^2(n_j + 1) \\ & + h_1b_1V_{sup}(I_0e^{\left(V_{sup}/N_pVT\right)}\left(\frac{N_{CYC}}{f}\right)(n_j + 1) + h_2b_1E_{elec}(n_j) + h_2b_2(1 + \gamma)d_j^nE_{amp} \\ & + h_2\gamma b_2E_{elec} + T_{CH}V_{sup}[C_{CH}I_A + (1 - C_{ch})I_s + E_{actu}N_{act}]) \end{aligned}$$

3.2.2. HYBRID GENETIC WITH ACO FOR SECONDARY SERVER SELECTION

A combination of two metaheuristics specifically GA and ACO are greatly utilized in this research. GA confers to population based technique where initial population is arbitrarily created. Genetic assessment is further done by arbitrarily produced initial solutions. In addition, ACO algorithm is a population-based technique. ACO do not necessitate initial population when compared with CA which is regarded as constructive approach in which ants search for improved solutions directed by parameter termed as pheromone. Initially, pheromone is identical for every arcs signifying problem at starting. At each iteration, pheromone levels updating is done in all arcs; in arcs covered by increasing ant pheromone

level, whereas in abandoned arcs it it evaporating). Consequently, elements signifying improved solutions receive additional pheromone than others and are further necessary in a subsequent iteration. In hybrid algorithm, solutions constructed (proposed) by GA are regarded as solutions attained through ACO in certain preceding iteration, and utilized for specifying initial pheromone level in solution graph. The solution is searched using ACO algorithm.

In the experiment, proposed hybrid method performance is compared to simple methods, both GA as well as ACO. A compatible chromosomal representation ought to be designed in a better way which should be utilized by GA and GACO. For that reason, Binary representation is selected in reasonable manner. Such solutions are guaranteed by these representations which are attained through a valid classical operators. Special operators are not defined for these representations.

1. Every chromosome comprises (n-1) groups of gene. 2. Number of genes in i th group is equal to (n-i) bit, so that total number of genes (N_{gen}) in chromosome follows equation (1).

$$N_{gen} = \sum_{i=1}^{n-1} i$$

The chromosomal representation is exhibited below

$b_{1,1}$	$b_{1,2}$	..	$b_{1,n-1}$	$b_{2,1}$	$b_{2,2}$	..	$b_{2,n-2}$	...	..	$b_{n-3,1}$	$b_{n-3,2}$	$b_{n-3,3}$	$b_{n-2,1}$	$b_{n-2,2}$	$b_{n-1,1}$
1				2						n-3			n-2		n-1

The processing flow of hybrid GA with ACO is given below:

1. Begin

2. Initialize first node of each ant

3. Finding the energy level of each ant according to equation 2 and for chromosome

4. Determining the node that accompanies high level of energy

5. Revise: Optimal node of each cycle, best solution and pheromone matrix and subsequent population with GA operator

6. n_cycles = n_cycles +!

7. Repeat until converges with end criterion

3.3. ANONYMOUS AUTHENTICATION PHASE

User anonymity is one which belongs to the imperative properties of two factor authentication strategies for WSNs. Accordingly, user un-traceability is considered being user anonymity's highly satisfactory property. In other words, this advance property is accomplished through a scheme, which is able to prohibit the adversary from connecting

several communication instances that have created by the single user, besides from monitoring a moving history, present location, etc. Consequently, numerous schemes, which predominantly tries to secure the user privacy tend to converge this robust notation of user anonymity. The subsequent steps describe the processing flow of anonymous authentication followed in this study:

- This is done by initializing the registration phase where all cluster members will share their temporal identity with the cluster head
- Here temporal identity is generated randomly by each cluster member which is not possible to guess by other nodes
- By using this temporal identity cluster head will generate the secret key which will be divided into two shares
- Here first share will be given to the corresponding cluster member and second share will be given to the secondary cluster head
- Thus no node can identify the privacy information of other users
- This secret information will be utilized for the authentication process

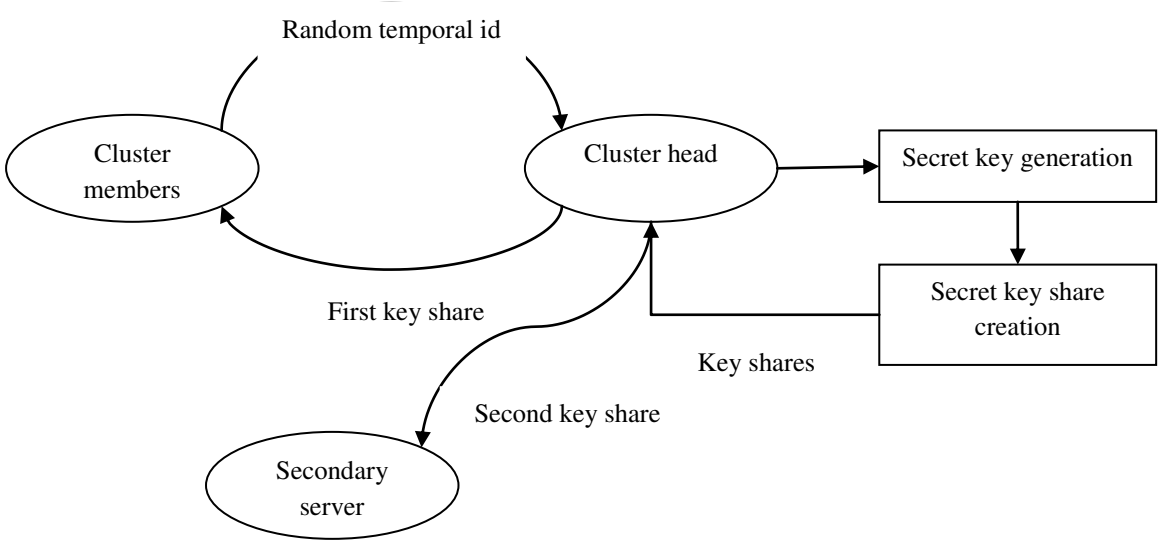


Figure 2. Processing flow of anonymisation authentication

3.3.1. RANDOM VALUE GENERATION PHASE

In this phase, each node in environment will generate their random number. This random number will be shared with the cluster head for further authentication process. A random number generator (RNG) refers to as a device that can generate a sequence of numbers/symbols, which is logically unpredictable through a random chance. In general, RNGs can be either of two types, namely Hardware Random-Number Generators (HRNG) or Pseudo-Random Number Generators (PRNG). Among that, HRNGs produce precisely random numbers. Whereas the numbers generated by PRNGs seem to be random, yet they are deterministic, besides they are able to be reproduced when the PRNG state is known. PRNG is nothing but an algorithm that generates the random number sequences by using

mathematical formulas. Through the approximation of the properties of random numbers, a sequence of numbers has produced by PRNGs. Using a seed state, PRNG begins from an arbitrary starting state. In the sequence, more numbers can get generated during the short span, if the starting point is known, besides it can get reproduced later. Therefore, the numbers have considered as effective and deterministic.

The evolution of computers makes the programmers recognize that the requirement of presenting randomness into a computer program is highly inevitable. Nevertheless, it is absolutely predictable, since the computer performs as per the provided instructions in an impulsive manner, so it is highly challenging to make a computer to execute such things by chance. As a deterministic framework, the computers do not generate accurately random numbers hence they have presented with PRNG method for generating random numbers..

The eldest and widely accepted algorithm for producing pseudo-randomized numbers is Linear Congruential Generator, which is described through the recurrence relation as follows,

$$X_{n+1} = (aX_n + c) \bmod c$$

where X is the sequence of pseudo-random values

m, 0< m- modulus

a, 0< a <m- multiplier

c, 0< = c<m- increment

x_0, 0<=x_0<m- the seed or start value

By using prior random integer, integer constants, and the integer modulus, the subsequent integer has generated. For initializing the function, an initial Seed has required that needs to be furnished by some means. The implementation of modulo arithmetic provides the randomness appearance. At this point, the generated random number will be provided to the cluster head to proceed further.

$$\text{Node} \xrightarrow{\text{PRNG } X_{n+1}} \text{ClusterHead}$$

3.3.2. SECRET KEY GENERATION AND SHARING PHASE

Consider X as a random value/symmetric key, which can be fed into an approved asymmetric-key pair generation algorithm as an input. Then, X shall be a bit string value of the subsequent expression,

$$X = U \oplus V$$

Here, a bit string of the desired length is denoted by U, which can be considered as an output of an approved PRNG. Besides. it can secure the target data by giving the support for required security strength.

• V is a bit string of the same length as U, and

• The value of V is determined in a manner that is independent of the value of U (and vice-versa).

Here, X will be utilized with the algorithm, through which the required bit length or/and the minimum security strength that can be provided by this utilization will get determined. An assumption is required by the conventional method, in which the selection of U gives maximum/all of necessitated entropy due to the non-restrictions over the selection of V (apart from its length and its independence from U). The requirement of individuality over U and V is computationally and statistically deduced, i.e. to compute U, the value of V is not necessitated, and, the value of U does not requires to compute V. Consequently, knowing one of the values (U or V) does not require to yield any information, through which an insight into the other value can be obtained. Consider U as the output derived by an approved PRNG, then the examples of independently selected values of V are as follows,

1. V is a constant (which is selected from the value of U in an independent manner). (Need to be remembered that if V is a string of binary zeroes, then K = U, in other words, it is approved PRNG's output).

2. V is a key that is derived through an approved key-derivation technique from a keyderivation key alongside other input which is independent of U;

3. V is a key which is generated in another cryptographic module in an independent manner. Subsequently, an approved key-wrapping algorithm is involved in securing V or an approved key transport strategy is employed to transport V in the following transport process. Once V reaches the key-generating module, its protection has removed before merging V with U as that generated U.

4. V is generated through hashing another bit string (V ′) by applying an approved hash function. Besides, before combining V with U, the result can be truncated to the suitable length for generating V (if required). In other words, V = T(H(V ′), k), in which the truncation of bit string x to its k leftmost bits is denoted by T(x, k), and the length of U is represented by k. The bit string V ′ can be one of the following factors, i.e. a constant; a key acquired from a shared secret throughout approved keyagreement strategy inside the key-generating module and another cryptographic module; or c) a key which was i) generated by another module independently, ii) transmitted through an approved key wrapping algorithm or transferred through an approved key transport method, and iii) the protection on the key was removed once it received.

3.3.3. AUTHENTICATION PHASE

In cryptography, Adi Shamir created an algorithm called Shamir's Secret Sharing. As a kind of secret sharing, a secret is partitioned in this algorithm, and giving each participant its own unique part. Subsequently, the least number of parts is necessitated to reconstruct the original secret. In general, all participants are required to reconstruct the original secret, but the threshold scheme requires lesser number of participants, which is lower than the overall count of the parts. Through Shamir's Secret Sharing, a secret is secured in a disseminated manner, which is used to secure other encryption keys frequently. Only a minimal number of shares is required to unlock the secret, if Shamir's secret sharing is utilized, which is called the threshold. Besides, it is used to represent the least number of shares required for unlocking the secret.

The goal is to split secret S (e.g. the combination to a safe) into n pieces of data S_1, ..., S_n can be defined as:

1. Knowledge of any k or more S_i pieces ease S to compute, i.e. from all combination of k pieces of data, the reconstruction of complete secret S can get carried out.

2. Knowledge of any k-1 or less S_i pieces leaves S completely undetermined, i.e. the possible values for S seem as likely as with knowledge of 0 pieces. In other words, the reconstruction of secret S is not possible if it is lesser than k pieces.

This procedure is termed as (k, n) threshold scheme. If k is equal to n, then each piece of the original secret S is needs to reconstruct the secret.

In our work only two pieces of secret key is generated and it is shared with the corresponding node and the secondary server. At the time of data communication this secret shares will be compared with each other and authentication decision will be made based on matching result.

IV. RESULTS AND DISCUSSION

Throughout this segment, the performance of the proposed Privacy concerned Anonymous Authentication Method (PAAM) has evaluated using NS-2 simulator. In this simulation model network, there are 100 nodes involved, which have randomly positioned within 100 × 100 meters area. In the simulations, the nodes are classified into two types, namely well-behaved nodes and malicious nodes, among which the malicious nodes possibly launch DOS attacks towards simulated circumstances. Whereas, the BS possesses unlimited energy. For a single interval, 10% of selected CH is set. During the simulation process, the proposed PAAM method is compared with earlier models, such as Latency and Power aware Reliable Intrusion Detection System (LP-RIDS), Prioritization Based Delay Avoided Secured and Reliable Data Transmission Method (PBDASRDT) and Attack Feature based Fast and Accurate Intrusion Detection System (AF-FAIDS) and prevailing LEoNIDS method [20] in order to assess the efficiency of the proposed method. Table. 1 depicts the parameters included in this research for analysing the reliability of the model. Through the subsequent metrics, namely packet loss, packet delivery ratio, energy consumption, end-to-end delay, and mean packet latency, the performance of PAAM system is evaluated.

Table 1 Simulation parameters

Simulation Parameters	Values
Channel	Wireless Channel
Mac	802.11
Antenna Type	Omni antenna
Routing Protocol	AODV
Initial Energy	100 joules
Traffic type	CBR
Agent	UDP

Simulation area	100X100 meters
Number of nodes	100

False alarm rate

A false alarm ratio (FAR) refers to the number of false alarms among the overall count of alarms/ warnings in a Sybil attack detection. In the following figure false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

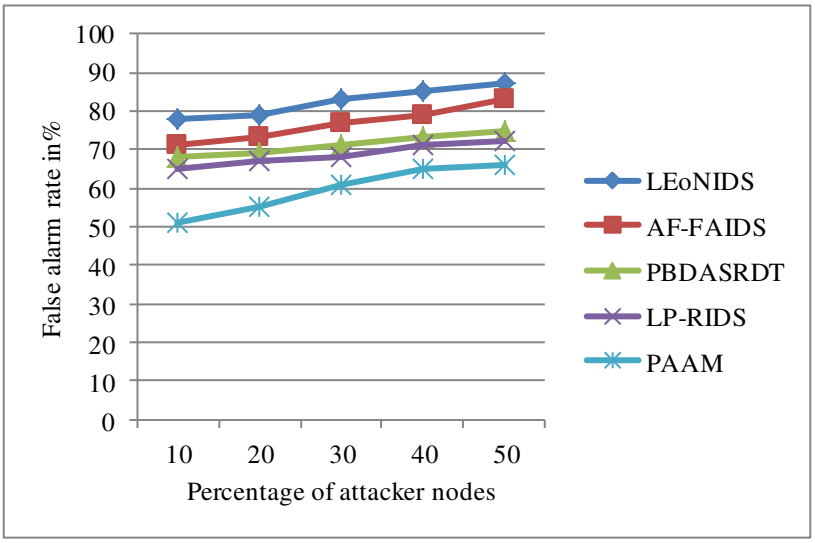


Figure 1. False alarm rate vs number of attacker nodes

Figure 1 compares the false alarm rate obtained for the proposed method and prevailing approaches. From the graphs, the proposed PAAM method tends to have better performance when compared to the previous techniques with lesser wrong detection of attacker nodes.

False positive rate

It defines the ratio between the number of negative events that have incorrectly classified as positive and the overall actual negative events. False-positive rate, which is the percentage that our algorithm incorrectly identifies the attacker node.

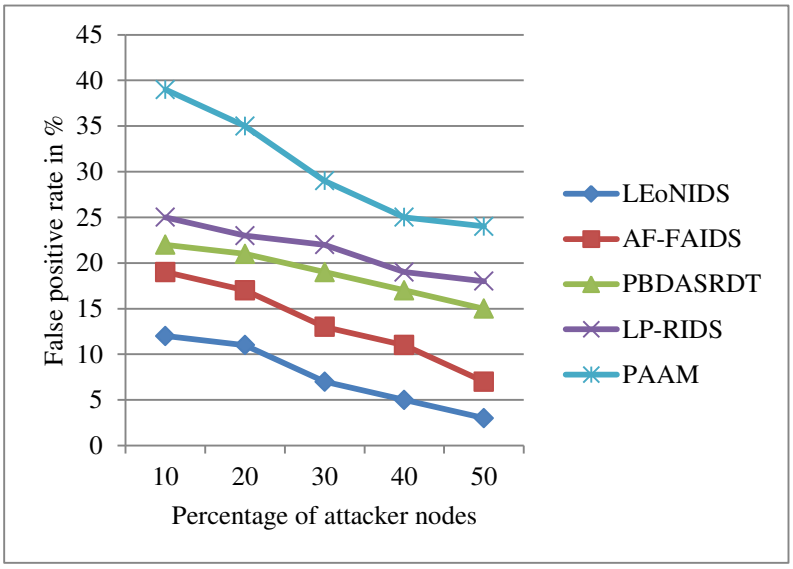


Figure 2. False positive rate vs percentage of attacker nodes

In figure 2, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. The graphs represent that the proposed PAAM method tends to have better performance when compared to the previous techniques with lesser wrong detection of attacker nodes.

Success rate Vs Ratio of colluding node

Success rate, which is the percentage that our algorithm can correctly identify the attacker nodes.

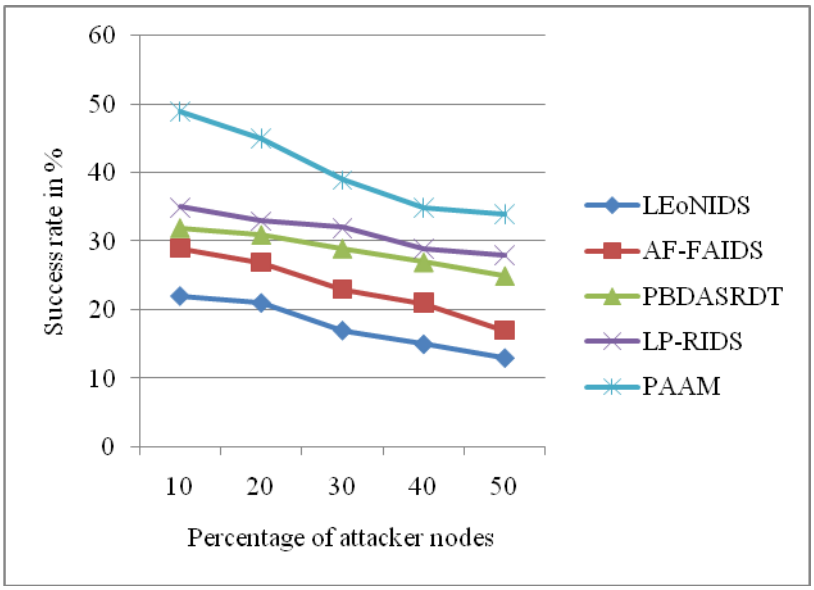
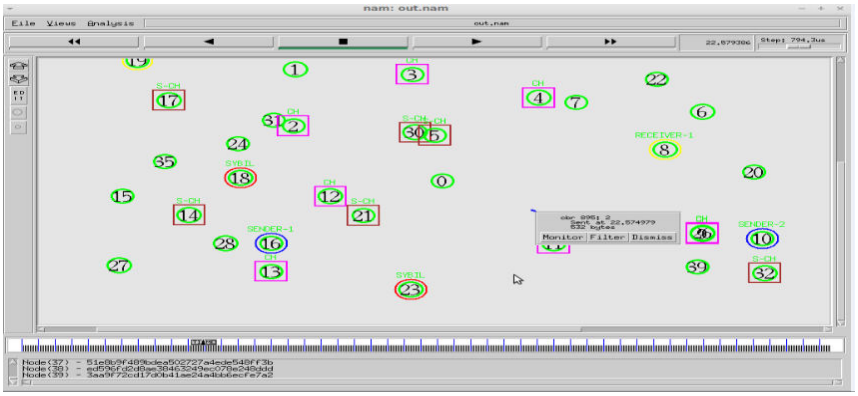


Figure 3. Success rate comparison

In figure 3, comparison evaluation of the success rate for the proposed and existing methodologies are given. The graphs depict that the proposed PAAM method tends to have better performance when compared to the previous techniques with accurate detection of attacker nodes.

Sybil attack probability Vs method

Sybil attack probability is defined as the effectiveness of proposed algorithm to capture the present of Sybil attacks from the total number of Sybil attacks. That is, it is the proportion of the number of captured sybils attacks and the total number of Sybil attacks present in the environment.



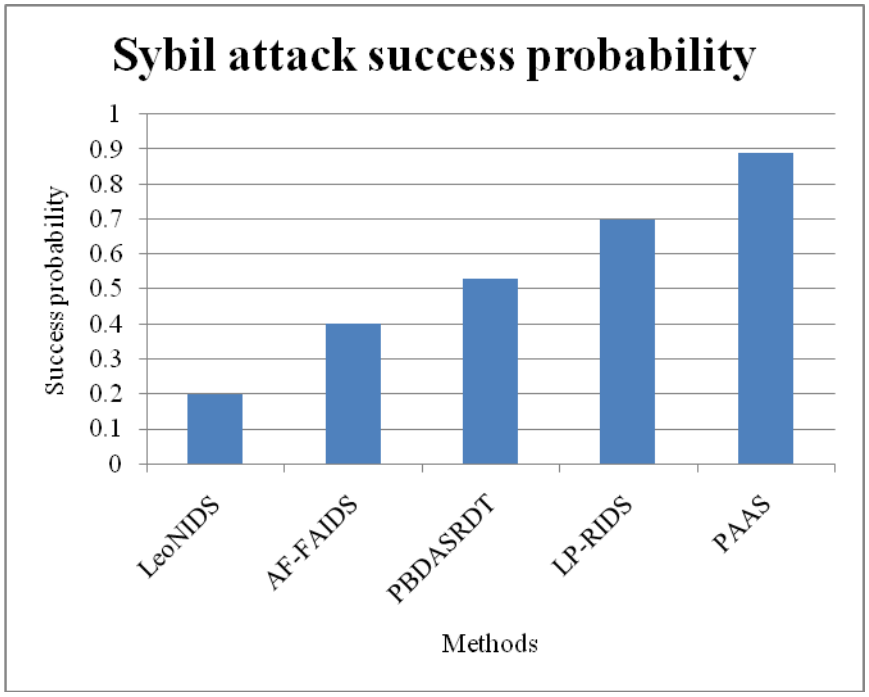


Figure 4. Sybil attack probability comparison

In figure 4, comparison evaluation of the success probability for the proposed and existing methodologies are given. From the graphs, the proposed PAAM method tends to have better performance when compared to the previous techniques with accurate detection of attacker nodes.

V. CONCLUSION

Throughout this study, Sybil attack prevention is ensured by introducing Privacy concerned Anonymous Authentication Method (PAAM). In this work, secondary cluster head selection is carried out by using Hybrid genetic with ACO algorithm. Here the secondary cluster head selection is done with the concern of higher energy value. The node that have energy lesser than threshold will not be considered for the Sybil node attack detection. And

then anonymous authentication is performed to detect the Sybil attack. This is done by initializing the registration phase where all cluster members will share their temporal identity with the cluster head. Here temporal identity is generated randomly by each cluster member which is not possible to guess by other nodes. By using this temporal identity cluster head will generate the secret key which will be divided into two shares. Here first share will be given to the corresponding cluster member and second share will be given to the secondary cluster head. Thus no node can identify the privacy information of other users. This secret information will be utilized for the authentication process. Secondary cluster head will verify the cluster members at the time of data communication with the help of first share of secret key. This research method avoids the Sybil attack presence accurately. The overall implementation of the research work is executed in the NS2 environment, which depicts that the proposed technique tends to provide better result than existing work.

REFERENCE

1. Kumar, A. (2017). Energy Efficient Clustering Algorithm for Wireless Sensor Network (Doctoral dissertation, Lovely Professional University).

2. Hammoudeh, M., & Newman, R. (2015). Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance. *Information Fusion*, *22*, 3-15.

3. Bouali, T., Senouci, S. M., & Sedjelmaci, H. (2016). A distributed detection and prevention scheme from malicious nodes in vehicular networks. *International Journal of Communication Systems*, *29*(10), 1683-1704.

4. Amish, P., & Vaghela, V. B. (2016). Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia computer science, 79, 700-707.

5. Abdullah, M. I., Rahman, M. M., & Roy, M. C. (2015). Detecting sinkhole attacks in wireless sensor network using hop count. Int. J. Comput. Netw. Inf. Secur, 3, 50-56.

6. Liu, Y., Bild, D. R., Dick, R. P., Mao, Z. M., & Wallach, D. S. (2015). The mason test: A defense against sybil attacks in wireless networks without trusted authorities. *IEEE Transactions on Mobile Computing*, *14*(11), 2376-2391.

7. Capossele, A. T., Cervo, V., Petrioli, C., & Spenza, D. (2016, June). Counteracting denial-of-sleep attacks in wake-up-radio-based sensing systems. In *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1-9). IEEE.

8. Ren, J., Zhang, Y., Zhang, K., & Shen, X. (2016). Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Transactions on Wireless Communications*, *15*(5), 3718-3731.

9. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, *2015*.

10. Neudecker, T., Andelfinger, P., & Hartenstein, H. (2016, July). Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)* (pp. 358-367). IEEE.

11. Talele, A. K., Patil, S. G., & Chopade, N. B. (2015, January). A survey on data routing and aggregation techniques for wireless sensor networks. In *2015 International Conference on Pervasive Computing (ICPC)* (pp. 1-5). IEEE.

12. Abbas, S. (2019, April). An Efficient Sybil Attack Detection for Internet of Things. In *World Conference on Information Systems and Technologies* (pp. 339-349). Springer, Cham.

13. Amuthavalli, R., & Bhuvaneswaran, R. S. (2014). DETECTION AND PREVENTION OF SYBIL ATTACK IN WIRELESS SENSOR NETWORK EMPLOYING RANDOM PASSWORD COMPARISON METHOD. *journal of theoretical & applied information technology*, *67*(1).

14. Dhamodharan, U. S. R. K., & Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, *2015*.

15. Dhanalakshmi, T. G., N. Bharathi, and M. Monisha, "Safety concerns of sybil attack in wsn," in science engineering and management research (icsemr), international conference on, pp. 1-4, IEEE, 2014.

16. Sarigiannidis, Panagiotis, Eirini Karapistoli, and Anastasios A. Economides, "Detecting sybil attacks in wireless sensor networks using uwb ranging-based information," expert systems with applications 42, pp. 7560- 7572, no. 21, 2015.

17. Sujatha, V., and Ea Mary Anita, "Detection of sybil attack in wireless sensor network," 2015.

18. Triki, Bayrem, S. Rekhis, and Noureddine Boudriga, "An RFID based system for the detection of sybil attack in military wireless sensor networks," in computer applications and information systems (wccais), world congress on, pp. 1- 2. IEEE, 2014

19. Pantazis, Nikolaos, Stefanos A. Nikolidakis, and Dimitrios D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: a survey," communications surveys & tutorials,IEEE 15,pp. 551-591, no. 2, 2013.

20. Roychowdhury, Sinchan, and Chiranjib Patra, "Geographic adaptive fidelity and geographic energy aware routing in ad hoc routing," in international conference, vol. 1, pp. 309-31, 2010.