International Journal of Engineering & Technology, 7 (4.19) (2018) 589-595

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Thwarting Sybil Attack by CAM Method in WSN using Cooja Simulator Framework

Prateek Singhal[1], Puneet Sharma[2], Sheenu Rizvi[3]

[1, 2, 3]*Dept. of Computer Science and Engineering, Amity University, Uttar Pradesh, India*
**Corresponding Author Email: prateeksinghal2031@gmail.com*

Abstract

In the area of IoT Sybil attack is vulnerable where the fake identities can manipulate or misuse pseudoidentities to negotiate the successof spam and Internet of Things. The nodes illegitimately claim multiple identities against sensor and Ad-Hoc networks. The hostile or faulty remote computing elements faces the security thread on large- scale peer-to-peer systems. We have a trust agency to certify the identities prevent from the "Sybil Attack". Multiple identities that control sustainable fraction of systems so prevent from loss of information while data exchanging via networks or internet.In this paper the proposed CAM (Comparing and Matching) approach to prevent from Sybil attack by verifying the position of the sensors or node with their location ID. We match the ID of the node while data exchanging over network. We specifically given a complete assure security for WSN that these kinds of attack come out with unicast as well as multicast. We have practically analysis the simulation of network by gagingthe end-to-end delay, pack delivery and throughput of packets under the numerous circumstances to compute the effectiveness of packets. This simulation is on the erudite tool that is Cooja under a Contiki OS and highlight the security over data exchanging and exemplify the use feature for intrusion detection "Sybil Attack" in the Internet of Things.

Keyword: *IoT; WSN; Sybil attack; CAM; Position verification; Cooja.*

1. Introduction

Internet of Things which expands the outmoded internet to a modern ubiquitous network that connects the objects into the physical world. It starts fruition to develop the interaction between the peoples and objects. Whereas the IoT is firstly introduced by Kelvin Asthon at 1999 in MIT lab science centre and supply chain management [18]. IoT can senses the information by embedding the sensors on the object to collect the information from environment and our body via RFID techniques, sensor networks, wearable devices, etc [1-3].While there are various developing wireless communication techniques, like WIFI and short- range wireless communication, Internet of things enables users to share the information through others [4], [5] in internet of connected vehicles, wearable devices and social networks, etc [6], [7]. Internet of Things can bid various intelligent services that are used to form smart grid [12-14], smart home [11], smart city [16], [17] andsmart community [15] by integrating thecommunication, computation capabilities and sensing [8], [9]. Therefore, as the development of IoT technology is in highly progress there are the value-added requests flourish to simplify the people to get interact with the people, objects, and the world, and change the way of communication between each other's.

To enable the economically feasible solutions to a variety of application such as, traffic security, structural integrity monitoring and pollution sensing by the sensing networks which promise of new technology as the large subgroup of sensor networks application which entails security, if sensors monitoring the perilous infrastructures. Security is vital in the sensor networks and it is complexed by the broadcast fauna of wireless communication, and absence of tamper-resistant hardware.

Internet of things is vulnerable to Sybil attacks while developing, where fake identities can be manipulated by the attackers [19-21] or compromising the effectiveness of the system by manipulation of pseudoidentities. IoT system can generate the wrong reports, and user may get the spam and loses their privacy in the incidence of the Sybil attack. In the recent report [22] of 2012, there are the many sustainable accounts inveterate as a fake or Sybil account in social networks, total 76 million (approx. 7.5%) in Facebook, 20 million fake account are created as per the week on twitter.These Sybil account spread spam advertisement, malware and fishing website to grab or steal the user private information. Hence many of the Sybil attackers behaves same as a normal user to discover out whether an account is Sybil or not which is difficult and makes Sybil defence as a dominant importance in the Internet of Things.Sybil attack can be defied in three types; SA-1, SA-2, and SA-3 to refuge a wider range of prevailing Sybil attacks. SA-1 considered to have a partial number of connection with normal users, whereas SA-2 is difficult to eminent by using graph partitioned. SA-3 measured ina mobile network, where it is not easy to detect the graph information because it may or may not be available.

Fig. 1: Internet of Things

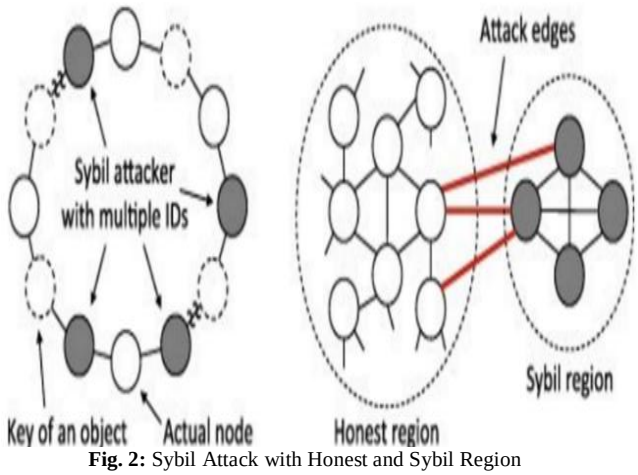


Fig. 2: Sybil Attack with Honest and Sybil Region

Sybil attack is pronounced by the Douceur in the content of peer-to-peer networks [23] in WSN and pointed out that it can conquest the redundancy mechanism of distributed storage system. Other authors Karlof and Wagner renowned that Sybil attack stances a threat toward routing mechanism in sensor networks [24].This is given by Brain zill working in Microsoft research labs [25]. Sybil attack only destroy the system environment of peer-to-peer by creating Pseudonymous and Sybil attack always deceitful nodes by showing the wrong location IDs or duplicate IDs of known people nodes in WSN. Whereas, a fault node enters in the network with different IDs know as Sybil node. There are many solutions to detect the Sybil attack such as Sybil guard [26], Sybil limit [27], watchdogs [28], path rate. In ad-hoc network also RSSI and channel-based detection for WSN [29]. The advantage for this scheme is that they are remarkably operational and can be reformed to advance the piece of the algorithm. Whereas detriment is that they can be higher before based on the model that can be a vulnerable to attack.

In this paper we have proposed a CAM method which is helpful in comparing and matching the location IDs and prevent from the Sybil attack which make fake IDs. CAM method is efficient and can reduce the time, cost and network size. We have stimulated this on the CONTIKI operating system which can be directly simulated the emulated on any hardware, this OS is very efficient and time saving, and we work on the COOJA tool which give the detection of Sybil node in the network.

2. Literature Study

- J. Dalfiah [31] et al propose the integration of efficient energy in meddling recognition system that discover the Sybil attack in network layer. In this he spots the node accuracy and elimination of false node which behaves like an original node.
- T. G. Dhanalakshmi [32] et al define the WSN sensors grid protection. Sybil attack is the most harmful attack in contradiction of sensors grid where normal besides the fake users can get entrance in the network unsuitably. To protect the date author projected the RAI (relate and identify tactic) and LVT (location verification technique).
- X. Zhenghong [33] et al it explicates the proposed protocol then the simulation results that can detect and guard against the routing attacks like WORMHOLE attack, HELLO attack and SYBIL attack.
- R. Vamsi [34] et al projected a LSDF (lightweight Sybil attack detection framework), divided into two, indication collection and indication validation. By evidence collection, it collects the evidence from each neighboring node by the help of activities and it can validate by broadminded proposition to select bordering node is a SYBIL NODE or else kindly node.
- Makhdoom [35] et al stretches a classified analysis on numerous defenses that was projected against Sybil attack. An innovative "One Way Code Attestation Protocol (OWCAP)" as he knows the weakness and strength of it, in wireless sensor network. This secure code assertation protect from the Sybil attack as it is economical, but it contradicts with maximum of the inner attacks.
- Y. Sun [36] et al projected the local indicator detection that is against the Sybil attack besides provide an operative solution. Firstly, RSSI-based detection which hold the address of the Sybil attack, secondly, it protects large number of node in the network from catastrophe that is instigated by Sybil attack and thirdly, by the help of executed experiment that preserve the probability detection with low system overheads that verified by RSDs.

3. Related Work

In network security Sybil attack is a critical apprehension which falsifies several fake identities to interrupt the network [37]. Sybil attack mostly occurred during the broadcasting and it involves deprived of discrete identity and verification assessment of each communication entity [38]. The attacker not only sending message to other nodes by different identities, but they also acquire more identities by merely disturbing the other nodes from dissimilar identities. In the system entity can be endeavouring to influence several set of entities are distinct by testing resource limit, but every entity is only aware of their different thought message over communication channel [37], [39] which is tough. To enhance the security in WSN the sensor node is fully organized by node establishment security, no dominant authority and node establish security is morally connected by the agreement.[49] The author binds the user's face and identity to use these SSCs for an attempt to resolve the impersonation and Sybil attack. While, these SSCs assume that these nodes are connected by infrared or wired connection [40]. Identities is tracked by the nodes which are often see together as contrasting to honest discrete nodes which moves freely in diverse direction. Where the node density is high there is also a high false positive isproduced.

3.1. Sybil Attack

When nodes or devices take unlawfully more identities which it does not imitate of one node which adopt identity of several nodes and making redundancy of routing protocol. The data integrity, resource utilization and security are always degraded by the Sybil attack [41].

Air resource allocation, storage, misbehaviour detection and routing mechanism are also performed by Sybil attack.

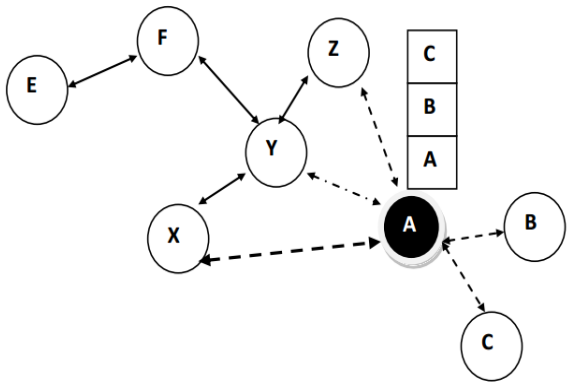


Fig. 3: Sybil Attack

There are hundreds of sensor nodes in the sensor network after the communication network. In between of wireless communication the sensor nodes pass over a central station and that nodes converse with stable number of nodes [42]. There are voluminous procedures accessible to encrypt the nodes from the external attacks, but the nodes also get mount on attack if they are inside the communication network. The insider attack is known as Sybil attack that can be detect in route, this is spoofing which is conducted by the ID of nodes in the network, and disturb the topology maintenance, geographic routing protocol in disseminated storing [43], [44]. In the Sybil attack spoofing of

node is done to another node that is called Sybil node (S) and the other one is normal node (N). In network announcement only, N node is to be communicated to each other, but here S node discriminate itself as centre known node and launches an attack in the communication network. In Sybil attack, Sybil node attempts to interact with their neighbour node by using the identity of normal node so multiple identities is present illegally to normal node in the network. The formation of Sybil node is done by stealing or forming of new legal identity so in the additional entity it presents as a misbehaving node or Sybil node in the network which make the network confuses and the network breakdowns. How the network can be attacked by Sybil attack classified below:

3.1.1. Direct attack and indirect attack:

The unique or normal nodes link directly with the Sybil node whereas in the indirect attack the communication is done via malicious node in it.

3.1.2 Simulation and Non-simulation attack:

The Sybil node contribute at the same time when the network start functioning the normal nodes.The number of devices in physical medium must be equal and the number of identities that are checked in cyclic manner. There is no method of different devices with different identities in different time in the network.
Whereas in non-simulation, a large number of identities can be control, generate and maintain by the malicious code on a single physical device and this gives a virtual impression to a network.

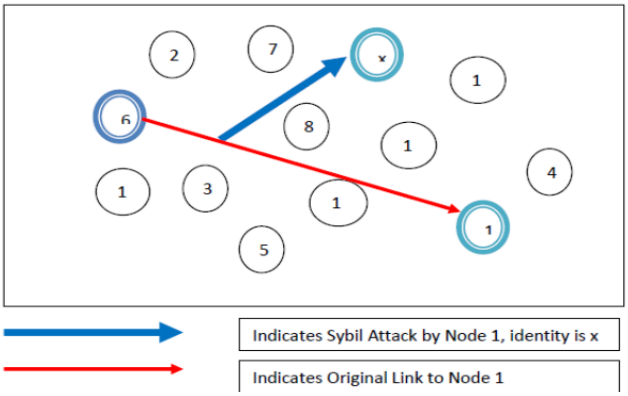


Fig. 4: System Model of Sybil Attack

3.1.3. Fabricated attack and stolen identity attack:

Illegal nodes are created by the use of legal identities of nodes. i.e., if sensor node has an ID of 16-bit integer then it generates same ID of 16 bit, then it is known as a fabricated node. The identity replication checker destroys the Sybil node that stolen an ID. The attacker with stolen identities discover the legal node and then uses it formalicious or hazardous attack. If the stolen ID is destroyed,then the attacker will become unidentified.

Table 1: Various form of Sybil attack that are vulnerable to protocols. *the non-simultaneous Sybil attack that are vulnerable to take votes over a potentially period of time. **joining is allowed in similar time intervals than resource allocated in this form of attacks. If the network flood is allowed only once per hour for nodes, but new nodes can join the network once per min.

	Communication		Identities		Simultaneity	
	Direct	Indirect	Fabricated	Stolen	Simultaneous	Non-Simultaneous
Distributed Storage	Yes	Yes	Yes	Yes	Yes	
Data Aggregation	Yes	Yes	Yes	Yes	Yes	
Misbehaviour Detection	Yes	Yes	Yes	Yes	Yes	Yes
Resource Allocation	Yes	Yes	Yes	Yes	Yes	Yes**
Routing	Yes		Yes	Yes	Yes	
Voting	Yes	Yes	Yes	Yes	Yes	Yes*

3.2. Sybil Attack in Social Graph

In IoT system if Sybil attack exist it do maliciously manipulation of data or information. The three types of Sybil attack in the social graph as we have shown below the social graph model. As G with n denoted the undirected graph, honest node(H) and total (E) edges with a (S) Sybil nodes.

In the real network the representation of identity, users and account is done by nodes in social graph. Social relationship is maintainedwith every pair of two nodes between edges with their weights.The connecting edge (BG) for Sybil node and honest one as shown below. The undirect social graph G is referred by social network said in some literatures [45], [46].

- **SA-1**

In the Sybil community SA-1 attackers build the connection usually that is Sybil nodes are connected tightly with other nodes. Social connection is built with honest nodes by the capability of SA-1but it is not strong enough. Whereas social connection between Sybil node and honest node are limited because the edge of SA-1 attack is limited. This attack usually exists between the social and sensing domain that are voting [47], OSN and mobile computing system [48]. It fully focusses on the manipulation of options and popularity. Sybil attacker's behaviour is indistinguishable from normal users.

- **SA-2**

This attack basically exists in the social domain but SA-2 can built a social connection with Sybil identities and also normal users. The perspective of social graph, normal users of social structure can mimic strongly in SA-2 with larger number of attack edges.
Main aim of SA-2 attack volatile users privacy, advertisement, disseminate spam and manipulation of malicious to the reputation systems for example OSNs. The main feature of SA-2 attack behaviour is that it can modelled as a Markov chain [49].

- **SA-3**

In the mobile networks or mobile domain there are SA-3 attackers with a same goal of SA-2 but impact of SA-3 within small period or local area.The connection cannot be established for long time or it may be intermittent between the mobile users due to of dynamics of mobile networks. At all the in the mobile network the centralized authority cannot be exists such as social relationship, historical behaviour pattern, global social structure, online system and topologies is not easy to obtain for Sybil defence toward SA-3 in the mobile networks. As compared to SA-2 and SA-2 in defence, SA-3 results in difficulties due to of lack of information and mobility.

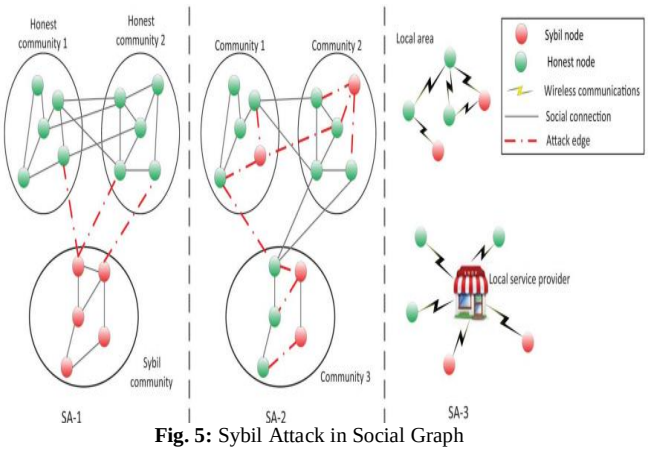


Fig. 5: Sybil Attack in Social Graph

Table 2: Sybil Attack description in Social Graph

Various Sybil attack	Social graph structures	Attack aim	Behaviour judgement	Mobility
SA-1	Exists in same region or community and Limited attack edges	Biased report or comment is uploaded maliciously	Normal user and frequently Specific behaviour is repeated	NO
SA-2	Connect tightly with normal users More attack edges	User privacy Dissemination spam Malware attack	High frequency behaviour purposely repeated	NO
SA-3	Normal user may be connected tightly with Sybil	Local popularity manipulation and spam in mobile environment	Specific behaviour frequently	YES

4. Proposed Work

In the wireless network it consists of WN nodes with a set of G= {wn_0, wn_1, wn_2, ……wn_i}, network G has a distinct sensors nodes wn_i. The data can be sensed within the region R from every node in the network. There are four levels in the system model, first level defines that every nodehas to register their location and IDs to the base station to record the stability in the network through sending Hello packet and it is being done in the initialization phase. Second level, due to increasing the size of the network it is necessary to place the nodes in the different sub-regions and classified it, while inter-region as well as intra-region [41] communication of the nodes is being done. Third level,in the other region a node can request the data from one region to another node in the region.
While communication the Sybil nodes is placed very near to the node that has requestedand it behaves like a requested node to

gather the information, location ID, node ID, data from the nodes, started acts as Sybil node known as Sybil attack. In the wireless network we can detect the Sybil attack by using or applying the CAM method and some remedy proposed.

CAM pseudo code:

1. Create anassembly of WN nodes.
2. These WN nodes would be connected by a link and each node is portable.
3. The head node is taken from one of the nodes.
4. H = {h_1, h_2, h_3,……, h_i,h_j,…,h_{wn}} // in the regions assigning by head nodes
5. While [h_i communicates with h_j]
6. If [key (node i) == key (node j)]
7. Data (node i) → node j
8. Qi ← source nodes position Є X, Y
9. Qj← destination nodes position Є X, Y
10. If ((mi (xi, yi) == Qi) and (nj (xj, yj) == Qj)) then
11. Mi sends data to Mj
12. Else display (“Sybil node”)
13. End if
14. End procedure

RSS Table Check pseudo code:

1. If: RSS-TIMEOUT
2. THEN: RSS_TABLECHECK ()
3. RSS_TABLECHECK ()
4. START_SUB:
5. FOR: For apiece address in the Table
6. DO:Pop_Element()
7. IF: (CurrentTime_getTime ())->Threshold_Time
8. Then:IF:getRSS()->Threshold_UB
9. THEN: Add_Malicious List
10. Else
11. Print” Normal out of Range”
12. End FOR:
13. End SUB:

In the network during the data traffic the CAM method is called because to check the information of nodes key from base station key information table. The information of current location of nodes is being gathered and checked by the original location information when we have created, this is done after the verification of node key information.While the attacker tries attack by changing its identity node, first it checks the previous identity node stored in the RSS table.At any point of time the nodes may get join and leave the network. A record of RSS histories is leaved by the nodes who gets exit from the network. RSS_TIMEOUT deletes the unwanted records and control the global timer, size when it plots in the algorithm. The RSS_TABLECHECK function is called when the timer expires and after it check the previous received RSS against TIME_THRESHOLD in RSS table for each address. If the time is obtained more than threshold that means it has more time elapsed from the previous node. The reason to find the RSS obtained is performed while checking against UB_THRESHOLD. If the previous identity attacker occurs then UB_THRESHOLD is large, otherwise it is the scenario of out of range.

5. Performance Evaluation

This system model is simulated in Cooja tool under Contiki OS with26 nodes and network size of 195mX195m. The sensor nodes behaving under AODV and under one base station for all node is constructed. To counter cloned or Sybil identities there is no mechanisms in RPL. In the figure shown below the ID 26 with purple colour indicated the cloned or Sybil identities. The downward path is represented by the blue arrow. The cloned or Sybil identities are visualized corrected as Cooja nodes from the downward paths. The black arrow, upwards route is chosen by one of the Sybil node as their parent and pointing toward leftmost Sybil nodes.The nodes can be traced until they cannot submit the authentication key values belong to the respective nodes.Through this paper we have compare before and after throughput of CAM algorithm included in the network to calculate the efficiency and network functionality. While we have stimulating to get the efficiency of network, reduce in network size, cost, etc. in the Cooja tool that is an erudite in nature to give the result accurate and it can be directly implemented on the hardware, works as a simulation and emulation. Firstly, we initialize the initializing window through VMware.
After this we have add the mote to the setup by mote->add mote->sky mote. The sky mote is efficient in the network simulation while sending or receiving the packets.

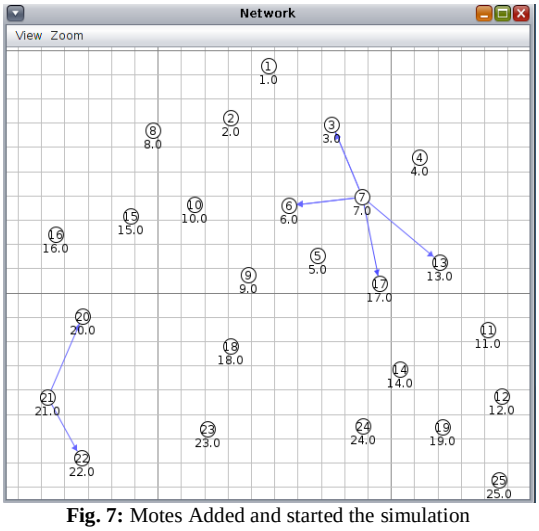


Fig. 7: Motes Added and started the simulation

After adding and start the simulation then the network graph is obtained as a result shown below

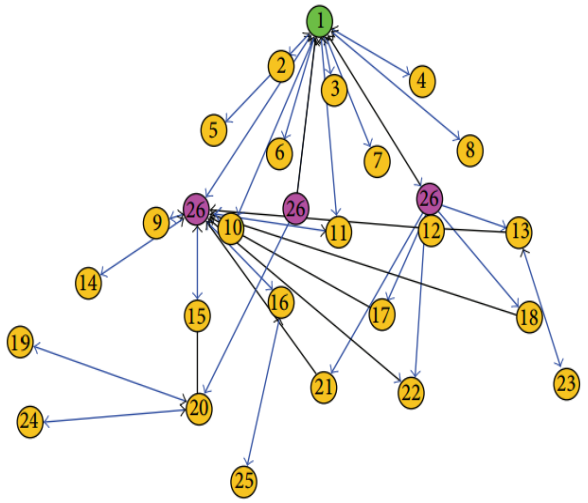
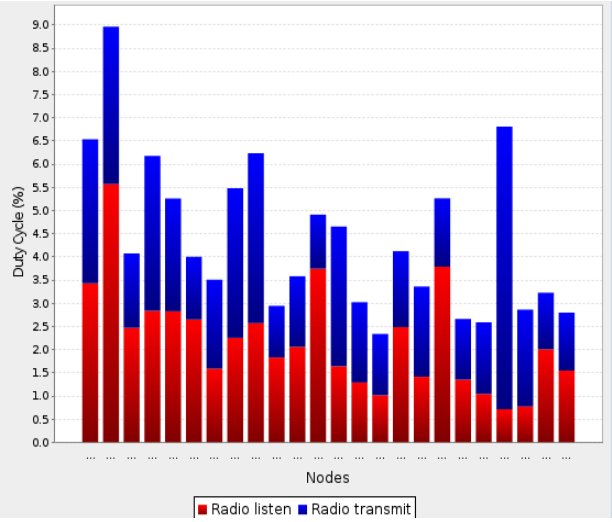


Fig. 8: Sybil Attack Network Graph

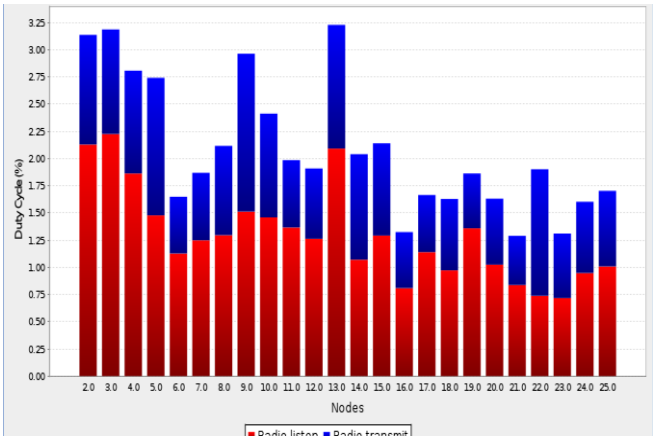
After and before comparison between the radio cycle of packet delivery as graph1 and graph 2



Graph 1: Radio cycle consumption Without using CAM method (9.0%)

By the graph 1: The target node gets the data packet within the time interval. If the data packet is received by the Sybil node then it sends the packet by changing its ID with same distance and data repeatedly.

By the graph 2: the CAM method is used for transferring the data packets with more efficient from different nodes in different time intervals.



Graph 2: Radio cycle consumption with CAM method (3.25%)

In the given figure 9 it tells about all the information of the nodes with all values such as ETX, LPM, NPM, Hops, etc.

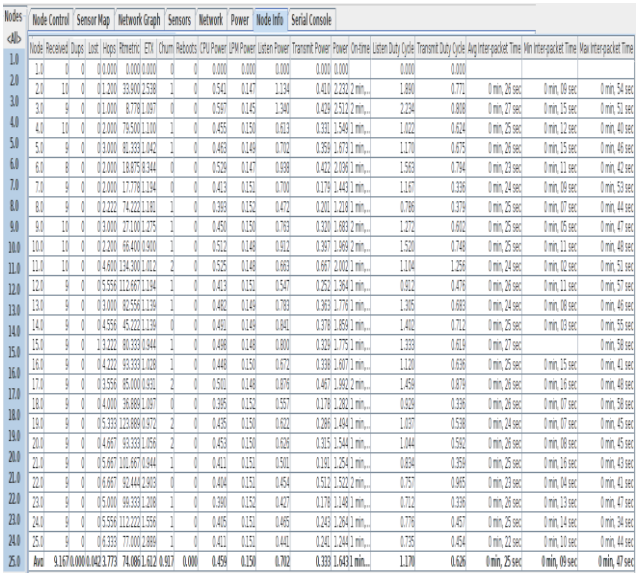


Fig. 9: Nodes Information

To check the network hops between the sensors while sending the data packets from one to another, it is shown in the figure 10.

This simulation is repeated by various number of time t for nodes and time in network, we get the optimized result with comparison output of CAM algorithm.

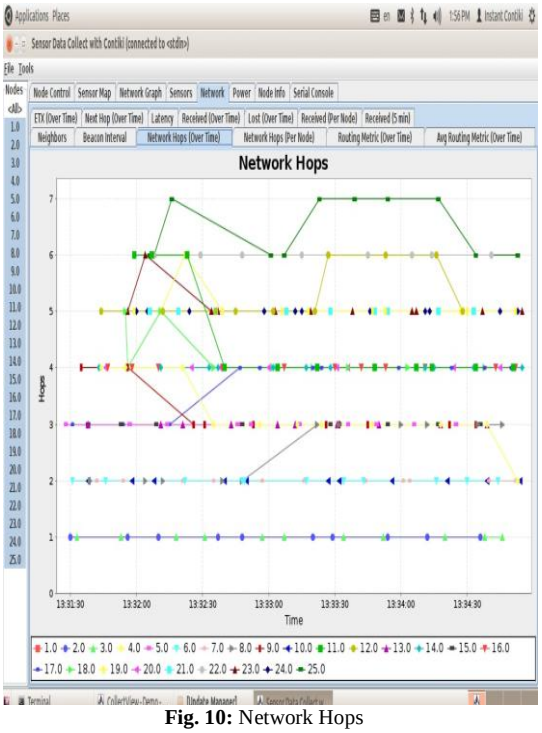
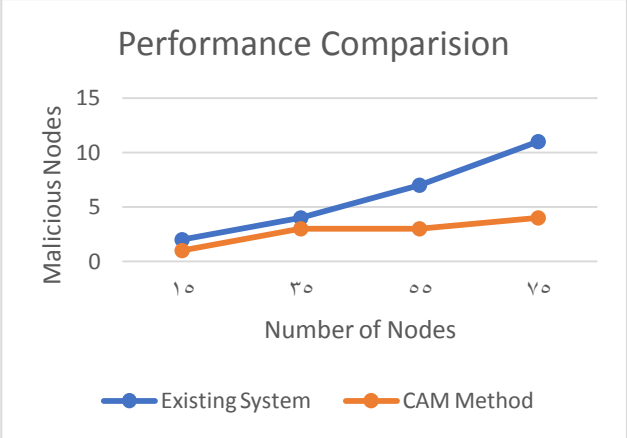


Fig. 10: Network Hops

Table 3: CAM-PVM comparison with multi rounds. (NN- Normal Node and SN- Sybil Node)

Method	Round 1		Round 2		Round 3		Round 4	
	NN	SN	NN	SN	NN	SN	NN	SN
Existing system	15	2	35	4	55	7	75	11
CAM algorithm	15	1	35	3	55	3	75	4

From the above table it is clear that while we use the CAM method it will give efficient result with minimum Sybil node rather that normal.



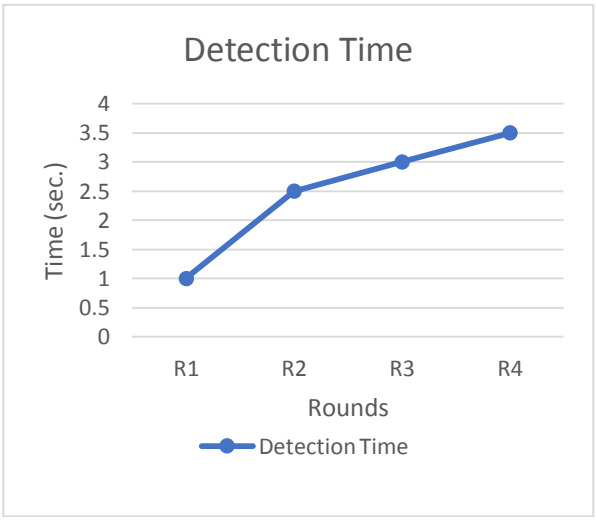
Graph 3: Number of Sybil node detection and Performance comparison before and after CAM method

The multiple round iscarried by the simulation where number of nodes are deployed in each round with different nodes and according to the normal node, the number of Sybil node are also varied. According to the first round we have deployed 15, 35, 55 and 75 nodes respectively. We have conducted the 4 rounds where it represents the existing system and CAM method for preventing the Sybil node in each round.

The performance is good in the CAM method as comparatively to normal existing system, but after some rounds the number of Sybil nodes will be constant. As per the round 1 out of 15 normal nodes while using existing system there are the 3 Sybil nodes but when we use CAM method then the Sybilnode is 1 and for round 2 out of 25 normal nodes using existing system then the Sybil node is 4 but using CAM method then 3, same process goes on till the round 4. In every round you see that when we us CAM the Sybil nodes is less rather than using existing system where the Sybil node is more.

Table 4: Detection of Time with respect to Time Slots

Round	R1	R2	R3	R4
Detection Time (sec.)	1	2.5	3	3.5



Graph 4: Detection of Time in each round

In the above Graph 4, in each round with particular Sybil node is being detected. The Sybil node are those nodes that acts like another node, due to making more communication it loses more energy while it communicates with the sources node to convey that it is a duplicate ID. The Sybil nodes can be detected by the location, response time and node id, as per the time period of Sybil node detecting is 0-1 sec in round 1, while in the period of 1.5-2.5 sec in the round 2 and in the period of 2.5-3 secthe round 3 and so on further time is getting increase which represent that in the network it controls the Sybil act as per the periods.

6. Conclusion & Future Work

In this paper the main work is to prevent from the Sybil attack in the WSN by using the CAM (Comparing and Matching) algorithm. It pretends as a Sybil node with replica ID and information, if and only if the node knows the whole information about the other node, it can be verifying the node by applying the CAM method. It cannot communication with other if it doesn't have the authorize permission by the base station or by the network. Rather than the old method, the CAM method is very effective and time consuming. In the future we can improve the CAM algorithm to reduce the cost, time in an effective way and network size will not be constraint. In the network throughput should be higher than other security algorithm that is applied before in the network security.

References

[1] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the Internet of Things," IEEE Commun. Mag., vol. 50, no. 12, pp. 144–149, Dec. 2012.
[2] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 6, no. 11, pp. 4136–4144, Nov. 2007.
[3] Y. Liu, K. Liu, and M. Li, "Passive diagnosis for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1132–1144, Aug. 2010.
[4] C. Tang et al., "Comparative investigation on CSMA/CA-based opportunistic random access for Internet of Things," IEEE Internet Things J., vol. 21, no. 1, pp. 33–41, Apr. 2014.
[5] O. Bello and S. Zeadally, "Intelligent device-to-device communication in the Internet of Things," IEEE Syst. J., to be published.
[6] L. Foschini, T. Taleb, A. Corradi, and D. Bottazzi, "M2M-based metropolitan platform for IMS-enabled road traffic management in IoT," IEEE Commun. Mag., vol. 49, no. 11, pp. 50–57, Nov. 2011.
[7] W. He, G. Yan, and L. Xu, "Developing vehicular data cloud services in the IoT environment," IEEE Trans. Ind. In format., vol. 10, no. 2, pp. 1587–1595, May 2014.
[8] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 414–454, May 2014.
[9] C. Lai et al., "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," IEEE Internet Things J., vol. 1, no. 1, pp. 46–57, Feb. 2014.
[10] H. Celdran, G. Clemente, G. Perez, and M. Perez, "SeCoMan: A semantic-aware policy framework for developing privacy preserving and context-aware smart applications," IEEE Syst. J., to be published.
[11] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A novel deployment scheme for green Internet of Things," IEEE Internet Things J., vol. 1, no. 2, pp. 196–205, Apr. 2014.
[12] A. Aziz, Y. Sekercioglu, P. Fitzpatrick, and M. Ivanovich, "A survey on distributed topology control techniques for extending the lifetime of battery powered wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 121–144, 2013.
[13] K. Zhang, R. Lu, X. Liang, J. Qiao, and X. Shen, "PARK: A privacy preserving aggregation scheme with adaptive key management for smart grid," in Proc. IEEE Int. Conf. Commun. China (ICCC), 2013, pp. 236–241.
[14] M. Wen et al., "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," IEEE Trans. Emerg. Topics Comput., vol. 1, no. 1, pp. 178–191, Jun. 2013.
[15] X. Li et al., "Smart community: An Internet of Things application," IEEE Commun. Mag., vol. 49, no. 11, pp. 68–75, Nov. 2011.
[16] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework of creating a smart city through Internet of Things," IEEE Internet Things J., vol. 1, no. 2, pp. 112–121, Apr. 2014.
[17] P. Vlacheaset al., "Enabling smart cities through a cognitive management framework for the Internet of Things," IEEE Commun. Mag., vol. 51, no. 6, pp. 102–111, Jun. 2013.
[18] K. Ashton, That "Internet of Things" thing, RFID Journal, 2009.
[19] Q. Lian et al., "An empirical study of collusion behaviour in the Maze P2P file-sharing system," in Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS), 2007, pp. 56–66.

[20] M. Yang, Z. Zhang, X. Li, and Y. Dai, "An empirical study of freeriding behaviour in the Maze P2P file-sharing system," in Proc. 4th Int. Workshop Peer-To-Peer Syst. (IPTPS), 2005, pp. 182–192.
[21] K. Zhang, X. Liang, R. Lu, and X. Shen, "Exploiting multimedia services in mobile social network from security and privacy perspectives," IEEECommun. Mag., vol. 52, no. 3, pp. 58–65, Mar. 2014.
[22] Business insider. (2013, Mar.). [Online]. Available: http://www.businessinsider.com/facebook-targets-76-million-fake-users-in-war-onbogus-accounts-2013-2
[23] J. R. Douceur. The Sybil attacks. In First International Workshop on Peer-to-Peer Systems (IPTPS '02), Mar. 2002.
[24] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, pages 113–127, May 2003.
[25] Liang Xiao, Student Member, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trapper," Channel-Based Detection of Sybil Attacks in Wireless Networks," IEEE Transactions on Information Forensics and Security, Vol. 4(3), Sep. 2009.
[26] Haifeng Yu, Michal Kaminky, Phillip B. Gibbon, Abraham D. Flaxman, Sybil guard: defending against Sybil via social networks, IEEE/ACM transaction on networking, jube 2008 vol. 16. P.576-589
[27] Haifeng Yu, Michal Kaminky, Phillip B. Gibbon, Feng xiao, Sybil limit: near optimal via social networks defense attack, IEEE/ACM transaction on networking, jube 2010 vol 16. P 885 -898.
[28] James newsome, Elaine shi, Dawn song, Adrian perrig the Sybil attack in sensor networks: analysis and defense.
[29] M. demirbas, y. song. An RSSI based scheme for Sybil attack detection in wireless sensor network. Proceeding of international of symposium world of wireless, mobile, multimedia networks (WoWMoM'06) 2006 p. 564-570
[30] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, A. S.K. Pathan, "A Novel Energy-Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks", 3rd International Conference onEco-friendly Computing and Communication Systems (ICECCS) 2014 IEEE.
[31] T. G. Dhanalakshmi, N. Bharathi, M. Monisha, "Safety concerns of Sybil attack in WSN International Conference on Science Engineering and Management Research (ICSEMR), 2014 IEEE.
[32] X. Zhenghong, C. Zhigang, "A Secure Routing Protocol with Intrusion Detection for Clustering Wireless Sensor Networks, "International Forum on Information Technology and Applications (IFITA), 2010 (Volume:1) IEEE.
[33] P. R. Vamsi, K. Kant, "A lightweight Sybil attack detection framework for Wireless Sensor Networks", Seventh International Conference on Contemporary Computing (IC3), 2014. IEEE.
[34] I. Makhdoom, M. Afzal, I. Rashid, "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks", National Software Engineering Conference (NSEC), 2014. IEEE.
[35] M. Li, Y. Xiong, X. Wu, X. Zhou, Y. Sun, S. Chen, X. Zhu, "A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013. IEEE.
[36] S. Sharmila1, G Umamaheswari2," Detection of Sybil Attack in Mobile Wireless Sensor Networks," Vol.2 (2), pp. 256 – 262, Mar-Apr 2012.
[37] Kuo-Feng Ssu, Wei-Tong Wang, Wen-Chung Chang," Detecting Sybil attacks in Wireless Sensor Networksusingneighbouring information," Computer Networks, Vol.53(18), pp.3042-3056, AUG 2009.
[38] Amol Vasudeva and Manu Sood," Sybil Attack on Lowest Id Clustering Algorithm in The Mobile Ad Hoc Network," International Journal of Network Security & Its Applications (IJNSA), Vol.4(5), Sep. 2012.
[39] S. Capkun, J.P. Hubaux, and L. Buttyan," Mobility helps peer-to – peer security," IEEE Transactions on Mobile Computing, Vol.5(1), pp. 43 – 51, Jan. 2006.
[40] Liang Xiao, Student Member, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trapper," Channel-Based Detection of Sybil Attacks in Wireless Networks," IEEE Transactions on Information Forensics and Security, Vol. 4(3), Sep. 2009.
[41] A. V. Pramod, Md, Abdul Azeem, M. Om Prakash," Detecting the Sybil Attack in Wireless Sensor Network," International Journal of Computers & Technology, Vol. 3(1), AUG. 2012.
[42] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons and Abraham D. Flaxman," Sybil Guard: Defending Against Sybil Attacks via Social Networks," IEEE/ACM Transactions on Networking, Vol. 16 (3), June 2008.
[43] Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, and Feng Xiao," Sybil Limit: A Near-Optimal Social Network Défense Against Sybil Attacks," IEEE/ACM Transactions on Networking, Vol. 18(3), June 2010.
[44] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman, "Sybil Guard: Defending against Sybil attacks via social networks," IEEE ACM Transnet., vol. 16, no. 3, pp. 576–589, Jun. 2008.
[45] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "Sybil Limit: A near optimal social network defense against Sybil attacks," IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 885–898, Jun. 2010.
[46] D. Tran, B. Min, J. Li, and L. Subramanian, "Sybil resilient online content voting," in Proc. USENIX Netw. Syst. Design Implement. (NSDI), 2009, pp. 15–28.
[47] Y. Reddy, "A game theory approach to detect malicious nodes in wireless sensor networks," in Proc. 3rd Int. Conf. Sensor Technol. Appl. (SENSORCOMM), 2009, pp. 462–468.
[48] G. Wang et al., "You are how you click: Clickstream analysis for Sybil detection," in Proc. 22nd USENIX Security Symp., 2013, pp. 241–255.
[49] S.V. Manikanthan, T.Padmapriya, "United Approach in Authorized and Unauthorized Groups in LTE-A Pro", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 10-Special Issue, 2018, pp. (1137-1145).