RESEARCH ARTICLE OPEN ACCESS

Detecting and Preventing Sybil attacks in Wireless Sensor Networks Using Message Authentication and Passing Method

Shrutika Gawandi[1], R. B. Ingle[2],M.R. Gurme[3]

Department of Computer Science and Engineering N. B. N. Sinhgad College of Engineering
Solapur -India

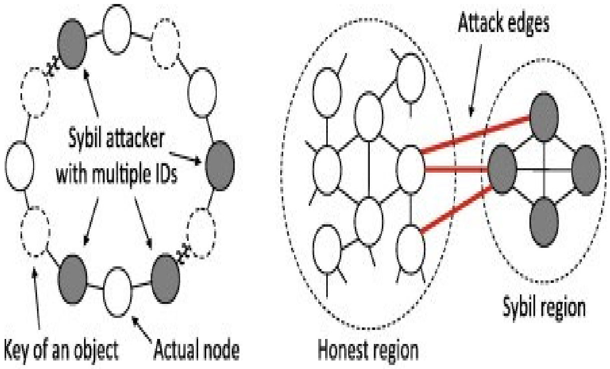
Abstract:

For secure set-up protection wireless sensor networks are highly necessary. In wireless sensor network till now a lot of researchers have predictable a choice of kinds of highly important attacks. A massive destructive attack against the sensor set-up where frequent genuine identities with fictitious identities are used for getting an banned entry into a complex is what a Sybil attack is. In wireless sensor set-up, discerning the Sybil attack, sinkhole and wormhole attack while multicasting is a fantastic job. A node which pretends its identity to other nodes is basically what a Sybil attack resources. Thereby Communicating to an banned node results in data loss and becomes risky in the set-up. The existing method Random Password association has only a scheme which just verifies the node identities by analysing the neighbours. With the objective of resolving this trouble a survey was done on a Sybil attack. For detecting, eliminating, and in due course preventing the entry of Sybil nodes in the set of connections a survey has been proposed by combine CAM-PVM (compare and match-position verification method) with MAP (message authentication and passing).To deal with the kinds of attacks in unica sting and multicasting we suggest a scheme of assuring security for wireless sensor network.

Keywords :- **Sybil attacks ,Message Authentication ,Networks Using Message**

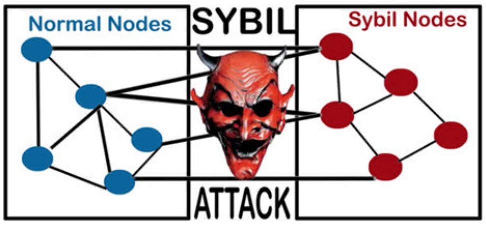
I. INTRODUCTION

Wireless sensor network is scattered self-directed system, gathering of antenna node that has heavily deployed through the ecological occurrence like physical, chemical and biological so which has cleanly sensing and communicating analysis by property. A wireless sensor network consists of applications such as green monitoring, target tracking, health monitor, and other various conservation options. Implementation and topology creation have become significant activities in modern explore work. The usage of wireless sensor network in a selection of applications is highly important with the emphasis on ensuring security. Still, avoidance and discovery of malicious attacks of all levels may be high or low in wireless antenna set-up. A multiplicity of attacks on the set of connections like wormholes, sinkhole, Sybil, sleep, and discriminating advance attacks in the network are being observed. Many researchers have well-known their own infrastructures which have convenient devices, used in various trade military in decentralized and scalable methods. Some of the devices are capable of synchronization not excluding the use of the internet for multiuser applications. They are used for finding the exact location in the algorithms that enhance the correctness. The Sybil attacker misleads other nodes by showing incorrect ID or copy ID of the users who are aware of the nodes in the wireless sensor network.



In the latest set-up position, alien nodes can become detectable in disguise in various identities and act as unusual nodes. Basically, there is no numerous master node in social and defense set-up for monitoring statement between system nodes intense. The analysis of peer-to-peer set-up shows that these networks show the existence of these network valid functionalities or the virtual networks Coventry exist, that is, the networks built on the top of other networks as in the internet. The network node addresses are based on the logical ID for structuring and forming networks.

[redacted]



[redacted]

The nodes in wireless antenna network are not in a fixed communications, whether single-hop, multi-hop communication, base position, gateways, and access points. Basically, wireless sensor network have a smaller transportation which could be non-infrastructure networks. The term ad hoc implies the establishment for a out of the ordinary purpose and for applications such as tracking, function rough calculation and edge discovery, monitor environment, and security domain in the motherland. The application of wireless antenna set-up, resembling a military force, monitors absence of restriction on the infrastructure as well as in the intermediary hop nodes.

This paper deals with one of the hazardous protection threats known as Sybil attack and proposes an algorithm known as meaning affirmation and passing method to hinder a Sybil attack in a wireless sensor set of connections.

II. ISSUES IN WIRELESS SENSOR NETWORK

The the largest part important issues that influence the design and management of a wireless sensor network are as follows:

1) Hardware and Operating System for WSN
2) Wireless Radio Communication Characteristics
3) Medium Access Schemes
4) Deployment
5) Localization
6) Synchronization
7) Calibration
8) Network Layer
9) Transport Layer
10) Data Aggregation and Data Dissemination
11) Database Centric and Querying
12) Architecture
13) Programming Models for Sensor Networks
14) Middleware
15) Quality of Service
16) Security

a variety of types of malicious activities are out-and-out in wireless sensor network. Some of these are created in expressions of nodes while others are produced in a network, data link, and application layers. Some are fashioned in the physical state.

The attacks are currently off the record as active and passive. The former is formed by operation of banned information in the set of connections that can affect it. Sybil, sinkhole, and eavesdropper are some of the dynamic attacks. Reflexive attacks are those which are meant to change the network assets such as lifetime and network size.

III. Attacks on wireless sensor network

A. Jamming: overcrowding node break off the entire system by chance because via the nature of inquisitive on radio frequencies, that it can be change the behaviour of node become an out of examination.

B. Collision: When node A have to communicate to node B at the same time node C be in touch to node B for transmit the data, In this case, shifting of packet communiqué in-between the nodes, signal collisions has been take place, it leads to not able to communicate with each other.

C. Selective forwarding attack: When node have to transmit the data by multipath navigation, in this mean time, any of the node may be compromise by the attacker node, expect if the node transmit the information by multiple nodes, in this mean time assailant could get the packets and which has reducing and transmitting the packets selectively. therefore it could not transmit the packets to correct path, at last it would not arrive at the correct objective.

D. Sinkhole: This type of attack that number of attacker nodes will be covers the certain region by incorrectly manipulated in sequence.

E. Wormhole: This category of attack has rerun assault, but this can bechanced into different part of the system

F. Sybil attack: At the same time, same node acts as special one. This is one of the main attacks. In this exchange, briefly converse about the Sybil assault, First, Its current the introduction of Sybil attack, creation of Sybil nodes, and types of Sybil attack. Second, it present some defence mechanisms.

Types of security attack:

There are two types of safety attack are present active attack and reactive attack. Active attack in which the attacker cause modification of data. There is physical damage in the network like variation of resources, alteration of data, changing traffic direction or work to rule of data to sink nodes. These attacks are simply special and we can stop the attackers as well as start the organization recovery procedure. There are four categories of active attacks are present masquerade, replay, alteration of messages, and denial of examination. A masquerade takes place when one entity pretends to be a different entity. A impersonate attack usually includes one of the other forms of active assault. Replay involves the passive capture of a data unit and its succeeding retransmission to produce an unauthorized effect.

Proposed Approach

The main intention of this paper is to design and increase an algorithm for detecting and preventing Sybil attacks in wireless antenna network. It is referred to communication authentication and momentary algorithm. establishment of Sybil activity through use of the other special identities is well known. Most of the existing make inquiries deals with the detection of the Sybil attack throughout confirmation of identities.

In this paper, N numbers of nodes are deployed in the system randomly under the organize of and an supervisor. These are well configured, energy efficient, and hopeful nodes in the network. During node conception, each node will receive a $HELLO$ message from the BS with a timestamp message representative the node establishment time (birth time) in the network. The entire node responds to the BS with a RES communication with ID, timestamp, and location. Then this information is stored in a $iNODEINFO\ table$ under the control of the supervisor of the network. The entire system model is presented as

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

where m is the digit of nodes in the network. Each node is deployed in the network as Location (Ni) = (rand (x), rand (y)), where X, Y is any location within the set of connections area. The BS sends a HELLO packet to all the newly created nodes in the network which can be written as

$$BS\ (\text{Msg}, \tau)\quad \sum_{i=1}^{m} Ni,$$

Where $N1,N2, . . . , Ni, . . . , Nm$ are Nodes. And, each node in the network is sending a RES packet to the BS which can be written as Ni RES BS, where the HELLO and RES packet consist of node ID and the timestamp. HELLO $=\tau(Ni)$ and RES = (ID(Ni), $\tau(Ni)$), where Ni denotes the ith node, $\tau(Ni)$ denotes timestamp of the ith node, and ID(Ni) denotes identity of the ith node. The parameters such as ID and τ are used to verify that the node is a Sybil or not. CAM-PVM algorithm for Sybil detection.

Compare and Match-Position Verification Method (CAM-PVM)

```
(1) $Let\ G = \{N1,N2,N3, . . . , Nm\}$
(2) $Let\ BS, Admin\ be\ the\ well\ configured\ nodes$
(3) $for\ i = 1\ to\ m$ // Nodes are placed randomly
(4) $Ni \leftarrow$ Location (rand($X$), rand($Y$))
(5) ID($Ni \leftarrow i$);
(6) $End\ Loop$
4 The Scientific World Journal
(7) Let Li be the set of link between pair of nodes in the network
(8) $Ni \rightarrow BS$(Msg, $\tau$)// For every nodes $Ni$
```

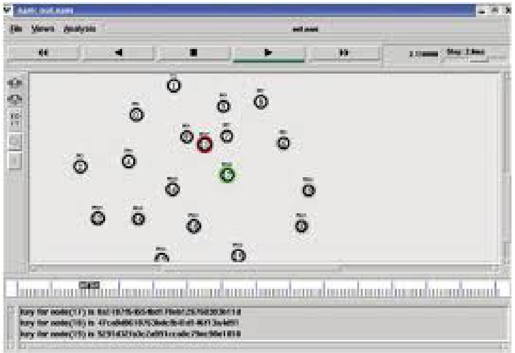
```
    $U* \rightarrow minimum$ distance $(Ni, Ni + 1)$
    $Ni\ RES\ BS$; $RES$ = ID, $\tau$, $X$, $Y$;
    $RES \rightarrow iNODEINFO\ table$
$End\ Loop$
$Su$ {U∗} $\rightarrow S$
$S \rightarrow RT(S)$
$Ni + 1 \rightarrow Ni(\tau)$
$\tau c$ = (ID, $X$, $Y$, $\tau$)
$U* \rightarrow D$
$for\ i = S\ to\ D$ //Route Discovery
    $RT$ $(S)$ $Ni$;
    Li $\rightarrow$ $(Ni$,$Ni$+1);
    $RES \rightarrow iROUTING\ table$
$End\ Loop$
$for\ i = S\ to\ D$// Data transmission
    $if(current\ Ni.info$ ==iROTINGtable==iNODEINFOtable)then
    $if\ (current\ Ni.info$==$iROUTINGtable$==$iNODEINFOtable)\ then$
        $Ni\ data\ Ni + 1$
    $else$
        $Ni + 1\ is\ blocked\ as\ Sybil\ Node$
$End\ Loop$
$iROUTINGtable$ entries clear
End
```

The CAM-PVM algorithm is used during the detection and data broadcast in the set of connections, where the node's in sequence is tartan from the BS $iNODEINFO\ table$.After confirmation of CAM-PVM algorithm, the algorithm collects the ID, timestamp, and modern place in sequence of the nodes and compares with initial information when they are registered. The results of the CAM-PVM algorithm can current only the trusted nodes in the way to make sure secluded data program. Otherwise the exacting nodes are treated as unknown nodes such as Sybil and data statement in the current is stopped and interchange path is chosen. Request of CAM-PVM is a time overriding method and also cost successful. So, that deterrence device is not compulsory in this paper to eliminate Sybil activity. Each node should be in touch by passing the confirmation message. In case the source node suspects the destination with dynamism, we can make use of the CAM-PVM with MAP algorithm for comparing and for communication confirmation to check whether the present node is Sybil or not. Where in the network G, a node Ni passes the data to node Nj the node Ni sends a appeal message to node Nj with its key, as msg(Ni), which is generate by the BS while registering in the network G.

Node Nj (destination node) submits its key memo with msg(Nj), and later, both keys are established by the base position and an ok indicate produced for sharing the data and any other in sequence. Data broadcast occurs between Ni,Nj once they get the signal from the base station. The pseudo code uses for the message verification and passing system are given below in detail.

Message Authentication and Passing (MAP)

```
$G$ = {$N0$,$N1$,$N2$, . . . , $Nn$}
$for\ I = 1\ to\ n$
    rtable = addrec($Ni$(id), $Ni(x)$, $Ni(y)$, $Ni$(msg))
    // node id, $x$, $y$ values of $i$th node
$End$
$for\ I = 1\ to\ n$
    $for\ J = 1\ to\ n$
        $Ni \rightarrow Send(request) \rightarrow Nj$
        $Nj \rightarrow Send(acceptance) \rightarrow Ni$
        $If$(msg($Ni$), msg($Nj$))$exists(rtable)$) then
            $Ni \rightarrow Send(dataP \rightarrow Nj)$
        $Else$
            $Choose\ the\ next\ neighbor$
        $End\ If$
    $End\ for\ J$
$End\ for\ I$
End
```



```
key for node(17) is [illegible]
key for node(16) is [illegible]
key for node(15) is [illegible]
```

Simulation of identifying Sybil node

Comparison of Sybil node with existing RPC method with CAM-PVM and MAP.

CONCLUSION

In this paper, we obtainable a brief survey on wireless antenna networks and safety issues. Then we discussed one of the most important attack- Sybil attack and set up classification of this attack. Sybil attack can exceptionally disrupt various operations of the wireless sensor networks such as assortment, data aggregation, data replication and data fragmentation, fair resource allocation scheme, misbehaviour discovery and routing mechanisms. Then we have also discuss different technique to alleviate Sybil assault.

Then the communiqué confirmation and passing process is applied for assessment the reliability or otherwise for a Sybil node. The action of a node as a Sybil node with reproduction ID and in sequence can happen only what time the node has complete in sequence about other nodes. Confirmation of the node needs the application of CAM-PVM. Instead of wasting time for CAM-PVM to check each and every node, the message substantiation and passing procedure is applied for authentication prior to announcement. If a node does not have any approval by the network or by the base station, it cannot be in touch with any other node in the network.

The message verification and passing system is so effectual and is known for more time overwhelming than any other method. Message verification and passing method requires amendment and reduction in time consumption and for cost competence. The size of the set-up is not a constraint. The throughput of the set of connections should be higher than the other safety measures algorithm which is applied earlier in the network safety.

References

[**1**] V. Rathod and M.Mehta, "Security in wireless sensor network: a survey," Ganpat University Journal of Engineering & Technology, vol. 1, pp. 35–44, 2011.

[**2**] A. Modirkhazeni, N. Ithnin, and M. Abbasi, "Secure hierarchical routing protocols in wireless sensor network; security survey analysis," *International Journal of Computer Communications and Networks*, vol. 2, pp. 6–16, 2012.

[**3**] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005.

[**4**]Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004.

[**5**] J. Newsome, E. Shi, D. Song and A. Perrig(2004), "The sybil attack in sensor networks: analysis & defenses," in IPSN'04: Proceedings of the Third International Symposium on Information Processing in Sensor Networks.

[**6**]R. Amuthavalli and R. S. Bhuvaneswaran, "Detection and prevention of sybil attack in wireless sensor network employing random password comparison method," Journal of Theoretical and Applied Information Technologygy.

[**7**] Yingying chen, "Detecting and localizing identity-based attacks in wireless sensor network", IEEE Journal, June 2010.

[**8**] D. Murat, and S. Youngwhan, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006. International Symposium, 2006.

[**9**] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary(2007), "Wireless sensor network security – a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press,

[10] Udaya Suriya Raj Kumar Dhamodharan1 and Rajamani Vayanaperumal2 "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method", The Scientific World Journal, Volume 2015 (2015), Article ID 841267, http://dx.doi.org/ 10.1155/2015/841267.