THE IIOAB JOURNAL
ARTICLE OPEN ACCESS

PRIOR ROUND REVEALS RSSI INFORMATION BASED SYBIL DEFENSE IN OPEN WIRELESS NETWORK

S.U. Akshaya*, D. Thilagavathi
Department Of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, INDIA

ABSTRACT

Aim: Open wireless ad-hoc network become harmful by possessing many identity which malicious node gains dis-appropriate influence and information. Many defense based on Sybil attack posed over channel estimation, trusted sources not exposed on the IEEE 802.11 network. The defense against the Sybil attack without any trusted authority is evaluated. Methods: RSSI observation and Sybil classification is performed with MASON TEST protocol with high computation in commodity devices. The method Prior round reveals RSSI information is implemented to reduce the computation time generated by the MASON TEST protocol. Novelty: Specifically, we implement the protocol and the method to defense against the Sybil attack, i.e. 99.99%, without trusted certification in minimum computation time. The performance is illustrated in network simulator and the result is analyzed.

Published on: 2nd -December-2016

KEY WORDS

Wireless network, Ad-hoc network, security, Sybil attack, Signalprint.

***Corresponding author: Email:** akshaya.cse004@gmail.com; **Tel.:** +91-9677340431

INTRODUCTION

Wireless network technology is one of the hottest topics in network fundamentals. Wireless networks serve many features. In various cases they uses cable replacements, where in other cases they are used to provide access to corporate data from remote location. The main four categories of wireless networks are WPAN (wireless personal area network), WLANs (wireless local area networks), WWANs (wireless wide area networks), and satellite networks. These networks are now commercially available in most of the region. The standards used in WLAN are 802.11 a, b, g, HIPERLAN/2. IEEE 802.11 is a combination of MAC (media access control) and physical layer (PHY) specifications for implementing WLAN (wireless local area network) computer communication in the 2.4 - 60 GHz frequency bands.

Wireless networks turns vulnerable to Sybil attacks, in which Sybil node poses identities in order to gain disproportionate influence. Various defenses based on localization of wireless channels exist, but something not exposed on commodity 802.11 devices. There introduces numerous security concern to defense against the attack, since participants are not vetted this assumption is easily broken by a Sybil attack. Defenses which are proposed falls into categories like trusted certification, social network based technique, misbehavior detection, resource testing, localization techniques. The trusted certification used access point or certification to vet participants, thus not useful in open nature of wireless network. Resource testing methods are most easily defeated in ad-hoc network of resource limited mobile devices by attackers with access to greater resources.

The localization technique supports defense mechanism against open ad-hoc network without trusted certification. RSSI (Received Signal Strength Indication) [1] is a localization technique uses the spatial correlation between the received signal strength and physical location of a node to identify the presence of a Sybil node. It is important to note RSSI does not relay on the quality of signal and usually an action is required for mapping RSSI distance values. In **Figure- 1 (a)** represents the RSSI observation from trusted APs used to identifies the Sybil's, where S is a Sybil presented by attacker M. Trusted RSSI observations, which are not generally available in open ad-hoc networks. In **Figure- 1(b)** represents the participant themselves act as observers. The observations areentrusted, coming from possible lying neighbors. In **Figure- 1**, (c) represents I believes S1 and S2 are falsified observation and incorrectly accept them and reject A and B as Sybil. A Signalprint [2] is used, as its direction stays unchanged; as RSSI can be changed by varying transmit power. Signalprint are hard to spoof and strongly correlated with physical location of nodes. Signalprints allow a control over Wireless Local Area Network to reliably single out clients. Instead of identifying clients based on MAC addresses or other data, Signalprints allow the system to recognize the identity based on how clients look like in terms of signal strength levels.

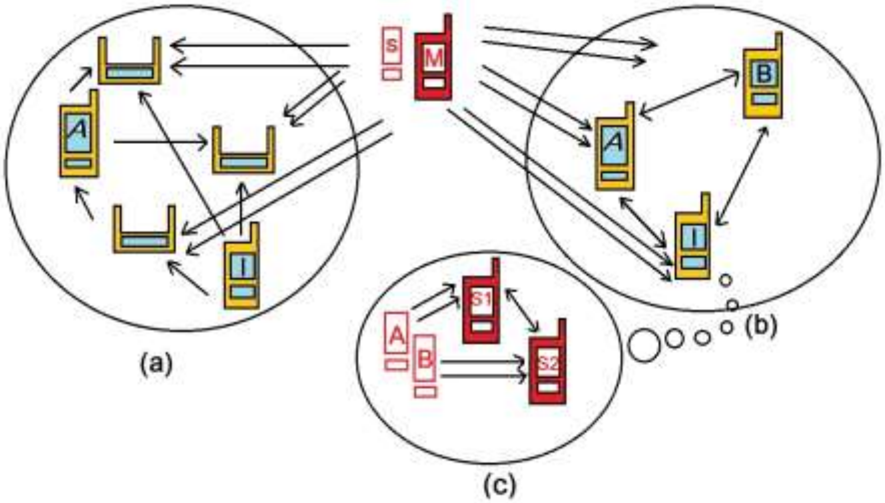


Fig:1. Trusted RSSI observation and false observations in Ad-hoc networks

……………………………………………………………………………………………

Murat Demirbas and Oguejiofor O.S noted that RSSI is a robust and lightweight solution for Sybil attack issue based client position in both indoor and outdoor environment. The framework naturally evaluates the distance between node hubs by measuring the RSSI (got signal quality marker) at a suitable number of node hubs.

The harmful attack against ad hoc networks is known as the Sybil attack. Sybil nodes refer to a malicious device's additional identities. Open nature of wireless network need a defense against Sybil attack, something exposed on commodity 802.11 devices. Without requiring trust in any other node or authority, RSSI is inherent use true or false RSSI observation reported by one-hop neighbors. The method prior round reveals RSSI information is used to reduce the computation time by comparing the RSSI prior round values. Performing Mason Test protocol with two components: collection of RSSI observations and Sybil classification. The protocol classifies non-Sybil and Sybil by vetting participants without using trusted authority.

RELATED WORK

Daniel B. Faria, (2006) uses signal print [3] technique to defeat against the sybil attack. The transmitting devices can be robustly identified by its signal print, a tuple of signal strength values reported act as sensors. The signal printcreates signal strength measurement is reliable to client idetifiers . The sybil clients can lie about their MAC address, signal print are strongly correlated with the physical location. Therefore, holding nodes with their Signalprints provides the proper matching rules. Signal print is featured in way that wireless network is able to detect a large class of effective DOS based on MAC address spoofing.

Murat Demirbas, (2003)[1][4] uses the RSSI as a solution to the sybil attack in wirless sensor network. The RSSI is said to be lightweight process, the issues like time-varying, unrelaible, non-isotropic is over come by using the Received Signal Strength Indication ratio. The RSSI is found to be the robust since it detects the sybil nodes with 100% completeness and less false positive ratio.

Mohamed Salah Bouassida, (2007) [5] reports that by collection of mobile host forming an estabilished infrastructure without aid. By allowing node to verify the authenticity of neighbour nodes based on the localization. To determine the estimated metric, the nodes are classified between the significance of the node.

Zhuliang Xu,(2013) [6] disscus about RSSI along with Ensemble Empirical Mode Decomposition (EEMD) and evaluate the performance in the indoor and outdoor environment. EEMD normalize the RSSI value related to the distance and reproduce the movement of the sender. EEMD can efficetivily ignore the RSSI value that changes in distance equation which is specific for one Wi-Fi devices. The EEMD along with RSSI is effective in outdoor thna indoor environment.Diogo Monica, (2009) [7] deploys a framework to evaluate the power and performance of radio resource test (RRT), i.e., each node has access to a single radio devices, the potential to support protocol that does not require pre-configuration nor pre-shares secret.

Yue Liu, (2013) [8] proposed a method Multiple-Input Multiple-Output (MIMO) [9] in Sybil defense by resource testing. In MIMO the received signal is validated to identify the transmission. The node is identified by multiple identities from same receiver to be a Sybil or malicious node. MIMO gains complete information about the received signal strength.

MATERIALS AND METHODS

In this segment, we summarize the problem, solution framework and briefly discus RSSI [5] and Signalprint methods.

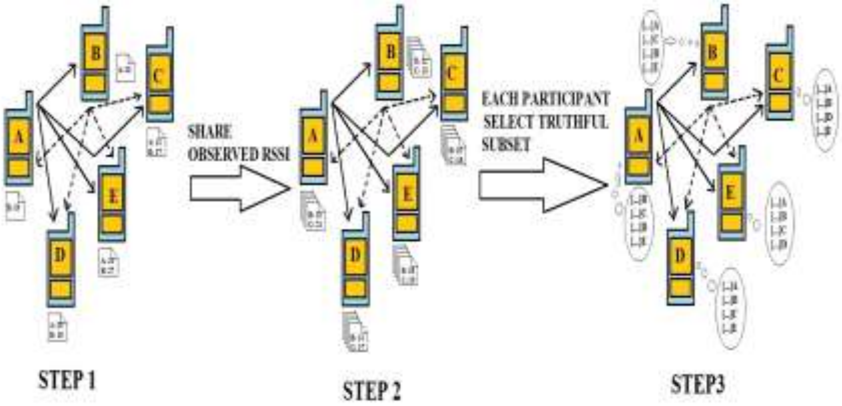


Fig. 2: Trustless truthful subset selection of RSSI observer

A. Problem Statement

We extent the Signalprint and RSSI based Sybil detection and classification methods to work without any prior detection or observation of participants to determine which of its one-hop neighbor are non-Sybil in open wireless network. The framework that formed allows us to identify the truthful subset selection of nodes for secure safe and trustful protocol.
The framework formed, **Figure- 2** illustrates truthful subset selection in three steps:

Step 1: First participant takes turn of broadcasting probe packet and other nodes record observed RSSI

Step 2: All the participant share their observation with their one-hop neighbors, i.e. each and every participant holds the RSSI observation of their one-hop neighbors.

Step 3: Finally each and every participant individually select a truthful subset for Signalprint base Sybil classification.

B. RSSI (Received Signal Strength Indication)

Received Signal Strength Indication [1] is a term of measuring the relative quality of the signal of the client nodes. The strength is based on the nodes signal as seen on receiving device, e.g. a smart phone. The strength of the signal is based on the distance and value of broadcasting power, at maximum broadcasting power the RSSI ranges from 40-50 m distance.

Deploying one node to transmit “hello” messages with constant power (i.e., 0 dBm) and another acts like receiver and capture RSSI then transmit them. The transmitter sends message over 1000 times by setting distance of 15 cm between the transmitter and receiver. But this deployment results to non-uniform nature of RSSI and poor correlation of RSSI value makes it unsuitable for Sybil detection. So, we deploy two receivers to compare ratio of RSSI instead of absolute value of RSSI[6] and observe the time varying of RSSI. By comparing the ratio, RSSI can take care of varied transmission power at sender. By using different transmitting power the sender broadcast 1000 messages. RSSI values are recorded by two receivers and transmit them to base station.

$$P_r(d)_{dBm} = R_{dBm} - 10nlog_{10}\left(\frac{d}{d_0}\right) + Z_{dBm} \quad (1)$$

Where,
R – Received Signal Strength Indication.
P_r – Received signal power.
Z – Gaussian distribution random variable with 0 mean value.
d – Distance difference betweenreceiver andtransmitter.

The base station analysis and compute the ratio of two RSSI values it received from the two receivers at time t1 and t2. The difference of RSSI ratio is calculated and logs this value.

This results in uniform distribution of values by following Gaussian Probability Distribution with standard distribution of 0.066 and 0.106, as in $equation\ (1)$. If D1 and D2 is the difference of RSSI ratio in same location and I1, I2, I3 and I4 are the node identity with a threshold.

$$\left(\frac{R_{I1}^{D1}}{R_{I2}^{D1}} - \frac{R_{I1}^{D2}}{R_{I2}^{D2}}\right) < \sigma, \left(\frac{R_{I1}^{D1}}{R_{I3}^{D1}} - \frac{R_{I1}^{D2}}{R_{I3}^{D2}}\right) < \sigma,$$
$$\left(\frac{\mathrm{R}_{\mathrm{I1}}^{\mathrm{D1}}}{\mathrm{R}_{\mathrm{I4}}^{\mathrm{D1}}} - \frac{\mathrm{R}_{\mathrm{I1}}^{\mathrm{D2}}}{\mathrm{R}_{\mathrm{I4}}^{\mathrm{D2}}}\right) < \sigma \quad (2)$$

It is safe to set σ as 0.1 and threshold to 0.5 to detected Sybil node 99.999%, i.e. the threshold to be 5σ, more specifically 0.1, calculated as in equation (2). **Figure- 3** represent the ratio compared between RSSI.

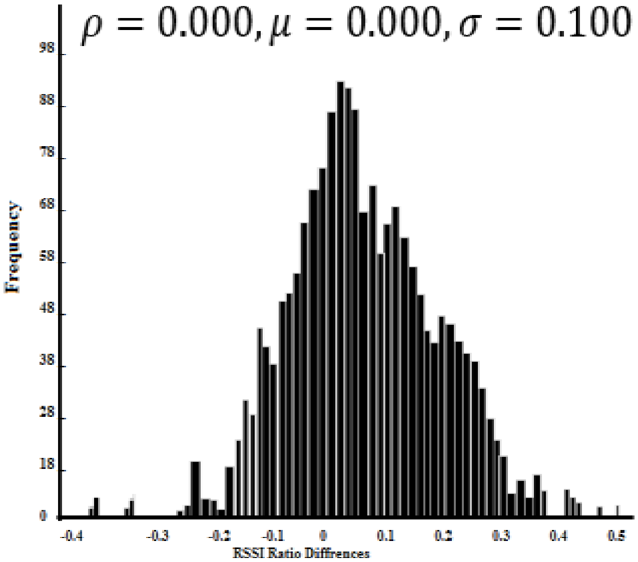


Fig. 3: Comparing ratio of RSSI

C. Signal print

THE IIOAB JOURNAL ISSN: 0976-3104

Signalprint [2] is vector of RSSI median. The properties of Signalprint are: Strongly correlated with the physical location with close proximity of client and Packet violently transmitted by stationary nodes generates similar Signalprint with high probability. Signalprint value can be written as original value or as relative value with respect to high and lower values of RSSI [9][12] levels in dBm. The difference between the value at an appropriate position and maximum values found in the Signalprint, is calculated using the term differential signal strength. When matching two Signalprint (i.e. S1, S2) it should be written with both absolute and differential values. The use of differential values increases the Signalprint operation that varying transmission power between the nodes.

MAX-MATCHES: By comparing the Signalprint (i.e., S1 and S2) the total number of $\in$ dB is found, denoted by (S1, S2, $\in$), i.e, 10-dB at position I and S1[i] and S2[i] are non-default values, as in equation (3).

If,

abs(S1[i]-S2[i]) $\leq$ 10 (3)

MIN-MATCHES: The Signalprint S1 and S2 is compared and the total number of $\in$ dB is found, denoted by (S1, S2, $\in$), i.e, 10-dB at position I and S1[i] and S2[i] are non-default values, as in equation (4).

If,

abs(S1[i]-S2[i]) $\geq$ 10 (4)

RESULTS AND DISCUSSION

The goal of the research is to defense against the Sybil attack without any trusted authority byminimum computation time by extending the Sybil defensemethod with Prior Round Reveals RSSI Information.

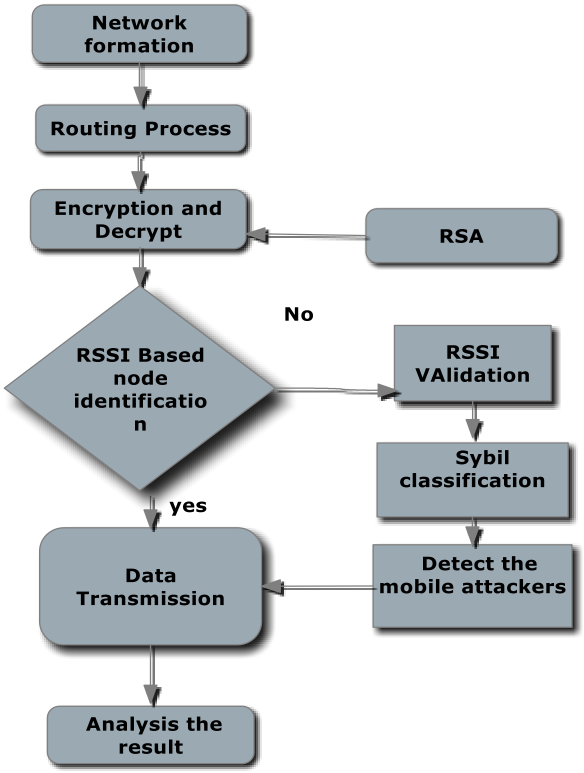
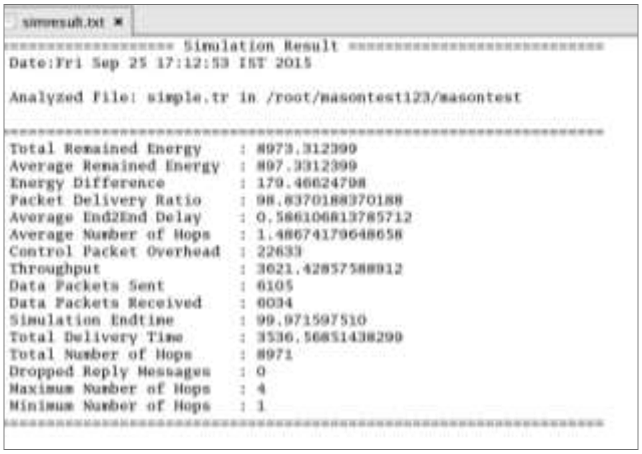


Fig. 4: Sybil Defense Mechanisms

Figure- 4 represent the flow of the defense mechanism. The resultant performance of the Mason Test along with the PRRRI method is evaluated and analyzed based on the simulation result as show in the **Figure- 5**.



```
==================== Simulation Result ============================
Date:Fri Sep 25 17:12:53 IST 2015

Analyzed File: simple.tr in /root/masontest123/masontest

===================================================================
Total Remained Energy    : 8973.312399
Average Remained Energy  : 897.3312399
Energy Difference        : 179.46624798
Packet Delivery Ratio    : 98.8370188370188
Average End2End Delay    : 0.586106813785712
Average Number of Hops   : 1.48674179648658
Control Packet Overhead  : 22633
Throughput               : 3021.42857588812
Data Packets Sent        : 6105
Data Packets Received    : 6034
Simulation Endtime       : 99.971597510
Total Delivery Time      : 3536.56851438290
Total Number of Hops     : 8971
Dropped Reply Messages   : 0
Maximum Number of Hops   : 4
Minimum Number of Hops   : 1
===================================================================
```

Fig. 5: Simulation Result

……..

A. Prior Round Reveals RSSI Information (PRRRI)

The method prior round reveals RSSI information is deployed to reduce the high computation time computed during MASON test protocol. The method is not actually the defense mechanism where as it is mechanism to reduce the time of computation time. Three steps of the PRRRI method are:

Step 1: Routing Process

The process of selecting the best path to transmit packets between nodes in the open wireless ad-hoc network in the IEEE 802.11. Distance vector routing protocol (DSDV)[10] is the routing protocol used as Routing process. In the 802.11 WLAN network the DSDV[11] operates by having each node *i* in the network by maintaining a table, which gives the best distance to each destination and which routes to get information with all its neighbors periodically. Each and every node has a single entry in routing table. The entry node will have following information of the nodes: IP address, lastest know sequence number and the hop count to reach the source node. Along with the details the routing table also holds the track of next hop neighbor to reach the destination node and the timestamp of the last update received for that node i.e., *DSDV_Agent::Update(int&periodic).* The updated message of DSDV consist of Destination address, Sequence number and Hop count. *DSDV_Agent:: updateRoute(rtable_ent *sequnum, rtable_ent *dstadd, rtable_ent *nxthop).* Each nodes deploys two mechanism to send out the DSDV update.s, they are: *Periodic updates*, *Trigger Updates.* When the update with same sequence number is received, the least hop count is given the precedence.

Step 2: Node certification

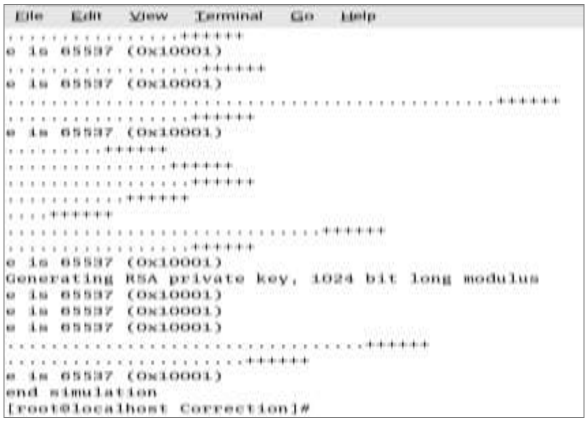
The node is certificated in two different ways: node id, certification id; by RSA cryptography. The generation of node id and certification id deploys the node to be highly secured. RSA generate the public key based on two large prime number must be kept secret. The prime number is large enough, so that someone without the knowledge of prime number cannot decode the message. **Figure- 6** represents the Node is certificated by performing RSA Encryption and Decryption, i.e., the certificated node denotes, PRRRI is performed.

Step 3: RSSI based Node identification

The prior round RSSI information is made an entry in to hash table and each every time the node is entering the network the Prior round RSSI information is initial step to process the node for data transmission as secure node. In the process of node identification after evaluation of routing process and RSA-Encryption and Decryption, the node is compared in the hash table with RSSI

THE IIOAB JOURNAL ISSN: 0976-3104

values that is performed in prior rounds, if the RSSI values compared in the Prior round that is updated in the hash table matches then the node does not processed with the MASON TEST protocol, if not comparison mismatches then the protocol is performed and data transmission is performed in open ad-hoc network. By performing every time the protocol will consume high computation time i.e., <5s for 5-10 nodes is typically fast but it is slower in high density area 40s for 100 nodes. Thus the method implemented reduces the high computation.



```
................++++++
e is 65537 (0x10001)
..................++++++
e is 65537 (0x10001)
.............................................++++++
.................++++++
e is 65537 (0x10001)
.........++++++
...............++++++
.................++++++
...........++++++
....++++++
.............................++++++
.................++++++
e is 65537 (0x10001)
Generating RSA private key, 1024 bit long modulus
e is 65537 (0x10001)
e is 65537 (0x10001)
e is 65537 (0x10001)
.................................++++++
......................++++++
e is 65537 (0x10001)
end simulation
[root@localhost Correction]#
```

Fig. 6: Result of Node Certification

……

The each time the new largest $\gamma -$ consistentsubset generated by the MASON test protocol iscarried with hash table to as prior round information.Each time all the participating identities entries the PRRRI the nodes information is compared with the prior round information of node i.e. RSSI ratio and identity classification. **Figure-7** represents the analysis of computational time reduction compared with prior work[13].

ALGORITHM 1: Node Verification.

```
Require:$(C, R_{max})$ is the $\gamma -$truthful consistence
h $\leftarrow$ $(C, R_{max})$
newhash = hashing(h, strlen(h))
Compute comparison between newhash with prior information.
if(newhash = hdr $\rightarrow$hashvalue)
    authenticate_result $\leftarrow$ MESSAGE_ACCEPTED
if newhash and (hdr $\rightarrow$hashvalue) not matches then
    authenticate_result $\leftarrow$ MESSAGE_ERROR-integrity violation");
end if
return newhash.
```

Node Certification Algorithm performs the comparison between the information of entry node and prior information of the same node.

B. The Mason Test

The Mason Test [13][15] is the protocol is implemented WLAN 802.11 to defense against the Sybil attack without using trusted authority. The protocol needs four main requirements:

1) The participating identities should be a conforming neighbors.
2) The examined packets should be transmitted in pseudo random order.
3) The information about the RSSI observation must not know to the attackers.

ISSN: 0976-3104

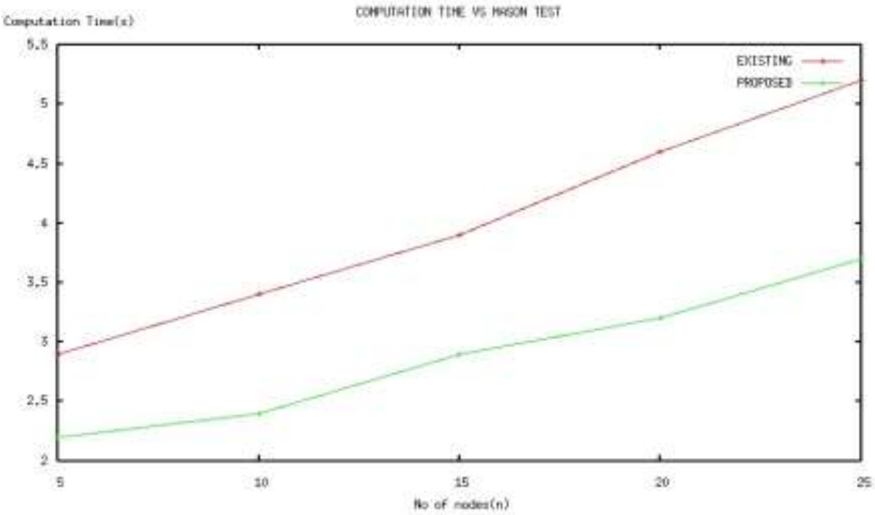
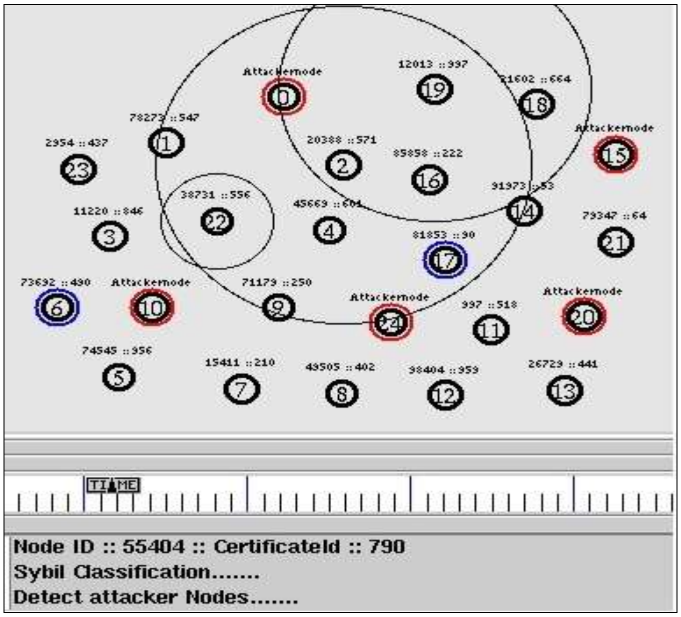


Fig. 7: Comparison of Computation Time

……..



Node ID :: 55404 :: CertificateId :: 790
Sybil Classification…….
Detect attacker Nodes…….

Fig: 8. Detect the Attacker Nodes

……..

The protocol performs two components: RSSI observation [14] and Sybil classification. At the end of the protocol results the nodes are classified in to Sybil and non-Sybil nodes.

1) RSSI observation

The RSSI observation is performed with three phases:

Phase I: Identity collection

The identities participating neighbors ensuring that none of the conforming identities are jammed by attackers are gathered in first phase, e.g. HI message is transmitted each acknowledged with initiator, unacknowledged HI is retransmitted. The process terminated if the channel stays ideal till timeout, all stationary neighbors respond with their own identities.

Phase II: Randomize broadcast request

In second phase the challenge-response protocol RSSI observation and Sybil classification for motion detection. E.g., the participant records the RSSIs of the HI message from the conforming identities. Some identities fails to

responds within minimum duration (i.e., 10ms) might be an attacker attempting to change the physical position and those identities are rejected.
Phase III: Report of RSSI Observation
In third phase first, each identity broadcasts a hash of its observation, then RSSI observation [4][16] values are shared, thus not matching the respective hash values are rejected. To prevent attacker from using the falsie observationvalues.

2) Sybil Classification
Sybil classification is performed by each participants individually. Correlation between the participants decrease with the RSSI values. The Sybil classification performs only with the current observation uncorrelated with the prior ones. In Algorithm 1, once the receiver set is chosen the set S contains a truthful receiver set is carried away to examine the -true Sybil classification. The Sybil and non-Sybil nodes are classified and the 99.99% of Sybil nodes are defended in the 802.11 WLAN ad-hoc network.

The goal of the candidate receiver set selection is, at least one of the candidate should be truthful. Size-n is set for desire receiver set, S is the truthful receiver set, R is the receiver set identity used to form the Signalprints[2]. Along with R the random element in the hash table, identities labeled non-Sybil by view V, i.e. V_{NS}(R), is updated to R. Truthful receiver set id updated with the new set {R}. Updated $\gamma -$truthful receiver set is compared with the number of identity whose RSSI [5][6] ratio reported by *I*do not match with *R*. the view generated by receiver set R VI and the view generated by all the participating identities and all Sybil identities i.e. V({i,s}) are not similar. The subset is found with new largest $\gamma -$ consistent the participating identities are classified as Sybil and non-Sybil identities. **Figure- 8** represents the result of detecting the attacker in open wireless network, named as Sybil nodes.

CONCLUSION

The Proposed work defense against Sybil attack in ad-hoc network without using any trusted authority. The use of trustless observation is made a significant improvement in detecting the Sybil nodes in the open wireless network. Signalprint method is one among the techniques of untrusted observation is deployed. We have proposed a method Prior Round Reveals RSSI Information to reduce the computation time generated by the MASON protocol. Conforming identities performs classification if their RSSI observations are correlated with the prior rounds. We deployed the RSSI to separate true and false observation of neighbor nodes. The protocol along with the method reduce the computation time compared to protocol deployed alone in IEEE 802.11 WLAN. The protocol robustly defense the Sybil node and method reduce the computation time of the protocol. The performance of the proposed work is analyzed in network simulator. For future work, the method is tested in outdoor and indoor environment and its performance is analyzed.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Murat Demirbas, Youngwhan Song, An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks, World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006.

[2] Daniel B. Faria, David R. Cheriton, Detecting Identity-Based Attacks in Wireless Networks Using Signalprints**,** WiSe'06, September 29, 2006, Los Angeles, California, USA.

[3] Daniel B. Faria, David R.[2006] Cheriton, Detecting Identity -Based Attacks in Wireless Networks Using Signalprints, WiSe’06, September29, 2006, LosAngeles, Calfornia, USA.

THE IIOAB JOURNAL
ISSN: 0976-3104

[4] IyadAldasouqi, WalidSalameh, Detecting and Localizing Wireless Network Attacks Techniques, International Journal of Computer Science and Security, 4(1).

[5] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky. [2009] Bertrand Ducourthial, Sybil Nodes Detection Based on

[7] Advanced Research in Computer Science and Software Engineering 3(8):. 5-10.

[8] D Monica, J Leitao, L Rodrigues, C Ribeiro. [2009] On the use of radio resource tests in wireless ad hoc networks, in Proc.3rd WRAITS.

[9] Y Liu, DR Bild, RP. [2013] Dick, Extending channel comparison based Sybil detection to MIMO systems, Tech. Rep. CSE-TR-584-13, Dept. of Electrical Engineering and ComputerScience, University of Michigan, Nov..

[10] MohitSaxena, Puneet Gupta, Bijendra Nath Jain. [2008] Experimental Analysis of RSSI-based Location Estimation in Wireless Sensor Networks, Communication Systems Software and Middleware and Workshops.

[11] Guoyou He. [2013] Effective Routing Protocol (DSDV) for Mobile Ad Hoc Network, International Journal of Soft Computing and Engineering (IJSCE), 3(5)

[12] Charles E. Perkins, Pravin Bhagwat, Highly Dynamic Destination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers, SIGCOMM '94 Proceedings of the conference on Communications architectures, protocols and applicationsPages 234-244.

Received Signal Strength Variations within VANET, *International Journal of Network Security*,9(1):.22-33.

[6] Zhuliang Xu, KumbesanSandrasegaran, Bin Hu, Cheng-Chung Lin, A Study of WLANRSSI Based Distance Measurement Using EEMD, International Journal of

[13] Madhusudhanan B, Chitra S, Rajan C, Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks, *The Scientific World Journal, Hindawi Publishing Corporation*, 2015.

[14] Yue Liu, David R. Bild. [2015] The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities**,** IEEE Transactions On Mobile Computing, V(99):2

[15] Giovanni Zanca, Francesco Zorzi, Andrea Zanella and Michele Zorzi, Experimental comparison of RSSI-based localization algorithms for indoor wireless sensor networks, REALWSN'08, April 1, 2008.

[16] Rajan C, Shanthi N. [2013] Misbehaving attack mitigation technique for multicast security in mobile ad hoc networks (MANET), Journal of Theoretical and Applied Information Technology, 48(3):1349–1357.

[17] Erin-Ee-Lin Lau, Boon-Giin Lee, Seung-Chul Lee, Wan-Young Chung. [2008] Enhanced Rssi-Based High Accuracy Real-Time User Location Tracking System for Indoor and Outdoor Environments, International Journal on Smart Sensing and Intelligent Systems, 1, (2).