Trust Aware Scheme based Malicious Nodes Detection under Cooperative Spectrum Sensing for Cognitive Radio Networks

Abhishek Kumar, Nitin Gupta and Riya
Department of Computer Science and Engineering
National Institute of Technology, Hamirpur
Himachal Pradesh, India

***Abstract*—Emerging of Cognitive Radio (CR) technology has provided optimistic solution for the dearth of spectrum by improving the spectrum utilization. The opportunistic use of the spectrum is enabled by spectrum sensing which is one of the key functionality of CR systems. To perform the interference free transmission in a cognitive radio networks, an important part for unlicensed user is to identify a licensed user with the help of spectrum sensing. Recently, the Cooperative Spectrum Sensing has been widely used in the literature where various scattered unlicensed users collaborate with each other to make the final sensing decision. This overcome the hidden terminal problem and also improve the overall reliability of the decisions made about the presence or absence of a licensed user. Each unlicensed user send the sensing results to the base station for final decision. However there exist some nodes which do not provide the correct sensing results to maximize their own profit which can highly degrade the CR network functionality. In this paper, a trust aware model is proposed for detection of misbehaving nodes such that their sensing reports can be filter out from the final result. The performance evaluation of the proposed scheme is done by checking its robustness and efficiency against various possible attacks.**

***Index Terms*—Cognitive Radio Networks, Cooperative Spectrum Sensing, Malicious Nodes, Primary User Emulation Attack.**

I. Introduction

In recent years, there is a rapid growth of wireless services which results in great demand of limited spectrum resources. The limited spectrum is divided into two bands i.e. licensed band and license-free bands. The utilization of licensed spectrum is inconsistent which plays a major role in the shortage of spectrum. Due to the fixed allocation scheme of the spectrum, the spectrum remains under-utilized and the unused spectrum is termed as spectrum hole. Recently, Cognitive Radio Networks (CRNs) has been used in order to improve the utilization of spectrum [1], [2]. Cognitive technology mainly focus upon opportunistic sharing of licensed band by secondary users (SUs) with licensed users termed as primary user (PU) without causing interference to them.

In spectrum sensing, few factors, such as shadowing and multipath fading may consequently deteriorate performance of PU detection by the SUs. Cooperative sensing improves the overall detection performance by aggregating the sensing results of the various SUs located spatially. Due to the spatial diversity the combined sensing decisions are more accurate than the sensing result of a single SU [3]. Generally centralized cooperative sensing is more beneficial in which the distributed secondary users forward their own results to the Fusion Center (SU BS), where the fusion center uses some fusion algorithms in order to combine the sensing results and decide about PU absence or PU presence [4].

However, in CSS mainly two security threats are faced by CRNs: First, PU emulation attack, the attacker act as the licensed user and the unlicensed user has to evacuate the spectrum band forcefully [5]. The second possible threat is spectrum sensing data falsification attack [6] where the malicious user provide false sensing report to the cognitive radio leading to wrong decision. On the basis of sensing reports produced by the malicious nodes, the attackers which provide the false attacks are classified into three types. The first type of attackers produce results in the form of yes (indicates that the PU is present when in fact it is absent) or no (indicates PU is absent when actually PU is present). The second type of user always produce sensing results opposite to the results they sensed, while the third type of users produce false results once in a while. These kind of false results which modify the final decision, results in false alarms where the SUs are prohibited to use the band by transmitting false information about the presence of PU, though in actual the band is idle. In the other case, the false results lead to the final decision, where it is concluded that the spectrum band is empty where it is in use.

In view of aforementioned problems, some security measures are required which ensure confidentiality(unauthorized users can not read the data on the network), integrity(detects changes in the data transmitted whether it is intentional or unintentional), availability(data is available to the authorized users whenever required) and access control(ensures that only authorized users can use the resources). In this work, cooperative sensing is considered where sensing results are influenced by the false spectrum sensing results by the malicious nodes. Therefore, in this paper a trust aware scheme for the malicious nodes detection is proposed such that these nodes are excluded during the preparation of final sensing report.

The rest of the paper is organized as follows. Next section discusses the work related to security in cooperative spectrum sensing. Section III discusses about the system model and

proposed scheme. In section IV performance of the proposed scheme is evaluated against various possible attacks in cooperative spectrum sensing.

II. Related Work

Survey of various threats on security in cognitive radio networks can be found in [7]–[10]. An algorithm is proposed by Wang et al. in [11]for the detection of spurious nodes in the network. The malicious nodes can be detected by calculating the trust factor and consistency factor for each users and the nodes whose trust values and consistency values were less than decided threshold value, were considered as the spurious nodes. The drawback of this method is that it considered that at single time only one attacker is active.

In [12], Noon and Li studied a new type of attack called hit and run attack, where the attacker can be in two modes i.e either it can produce the sensing report honestly or it can falsify the sensing reports. The author also found a method to mitigate this attack. In the proposed method, for each user, suspicious point value has been calculated and the threshold value has been decided such that when the suspicious point value of the user crosses the threshold value then it is considered as a spurious node.

For the detection of multiple spurious nodes in a system, Wang et al. [13], proposed a soft decision scheme in which the policy of attacker is assumed and the location of each user is known to the the base station. Heuristic approach has been used in order to identify the spurious nodes. Further, posterior probability has been used for the detection of suspicion level of each node. Then calculated probability was compared with the decided threshold value and if the value goes beyond the decided threshold value then the node is considered as malicious node. This approach is also known as "onion peeling approach".

In order to detect the data falsification attackers Bansal et al. in [14], made use of the signals generated by PUs in order to detect the nodes which were sending false signals. Similarly in [15], authors estimated the attack strength where the attack strength was considered as ratio of the number of spurious nodes to the total available nodes present in the network. Using this strategy, the authors estimated attack strength and used the Bayesian hypothesis for improving the performance of cooperative sensing.

In [16], Huang et al. considered the weight factor which depicts the contribution of user. Each user is allocated with some reputation and this reputation factor is negatively influenced by the fading. Mastui et.al. [17] also proposed an algorithm similar to the proposed method of Huang et.al. with the only difference that Mastui et. al. considered the distance between the two nodes where the location of SUs was assumed to be known to the base station.

Authors in [18], [19], proposed a mathematical model based on trust and reputation factor. Kar et al. in [20], used four parameters in their work in order to calculate the trustworthiness (sensing reputation). These factors were active factor, consistency factor, incentive factor and trust factor. On the basis of calculated trustworthiness the nodes are declared as spurious. However in order to apply trustworthiness factor it is necessary to detect the SUs successfully.

The proposed work considers trust value of nodes along with their previous reputation which is derived in the work. Only those nodes whose trust value and reputation values are above threshold are included in the sensing process and others are excluded.

III. Proposed Scheme

This paper considers the CRN consisting of a finite number of primary users, secondary users and a secondary base station which acts as fusion center(FC) [21]. The SUs wish to utilize the idle channel i.e. which are not currently being used by the PUs opportunistically. However, in order to use the licensed channel, a SU first performs spectrum sensing. The secondary BS and the SUs are assumed to be within the range of each other. The FC is used to collect the results of all SUs. First the secondary BS selects a channel from the network in order to perform sensing and then instructs the SUs to carry out sensing in the selected channel.The Common Control Channel(CCC) is used by the SUs in order to forward the sensing results to the secondary base station using one of the following techniques. In soft decision technique, parameters like measure of energy levels are calculated during SU sensing reports are send to the secondary base station by the SUs. Problem with this technique is that there is significant increase in the volume of communication data. While in case of hard decision, only one bit for decision making is used like '1' for presence and '-1' for absence of PU is send, and if the state of the channel is not clear then it is denoted by 0. Then suitable data fusion technique like OR, AND, MAJORITY rules etc. are used by the FC in order to make a final decision and then result based on the final decision is disseminated to all the SUs back.

It is assumed that SU base station itself is a sensing node. However, sometime it is not sure about its own sensing results. Therefore, while computing final sensing result, SU base station considers the confidence level ϕ. The overall sensing result produced by the base station for the channel is given by:

$$\chi_b = \phi\omega_{BS} + (1-\phi)\frac{\sum_{i=1}^{N}\psi_{ib}\omega_{ib}}{\sum_{i=1}^{N}\psi_{ib}} \tag{1}$$

where:

χ_b is the final sensing result given by base station for channel b.

ϕ is the confidence level of SUs base station.

ω_{BS} is the sensing result produced by the SU base station.

ω_{ib} is the sensing report produced by SU_i for channel b.

ψ_{ib} is the trust level of SU_i for the channel b.

N is the number of SUs having trust factor value greater than the decided threshold value for the channel b.

The threshold value is set to 0, whenever the variance in trust value in respect of a channel b for all the SUs is not considered and ψ_{ib} of all the nodes is set to 1. The equation

1 reduces to the average of sensing results obtained from the SUs in this case. Further, final decision D_b of made by SU base station is decided by the associated sign with final sensing result χ_b. Where, D_b is 1 if χ_b is positive, D_b is 0 if χ_b is zero and D_b is -1 if χ_b is negative.

A. Calculating Trust Value

In the proposed model, the assessment of the unlicensed users is done on the basis of last M behavior. The unlicensed user is awarded with[P,M] after each iteration and P,M $\epsilon 0, 1$. The unlicensed user is awarded with[1,0] if it provides accurate results whereas [0,1] if it provides false results. Further, two databases(trust and reputation databases) are used in order to store the sensing results,i.e. trust values and history. As it is well known that miss detection error has significantly more chances to occur as compare to the false alarms due to which trust and reputation factors of a SU are highly dependent on this. Further, forgetting factor (ρ_{kc}) is used in order to achieve the above mentioned goal and also stored with respect to each SU. The value of forgetting factor (ρ_{kc}) is ρ_1 if j is miss detection error otherwise the value of forgetting factor is ρ_2.

The value of trust factor for particular user in context c can be calculated as:

$$\psi_{kc} = \frac{\sum_{j=0}^{M-1} \rho_{jc}^{M-1-j} \mu_{jkc}}{\sum_{j=0}^{M-1} \rho_{kc}^{M-1-j} (\mu_{jkc} + \upsilon_{jkc})} \tag{2}$$

Where: $\psi_{kc}c$ is the value of trust factor of user k in the context c.

ρ_{kc} is the forgetting factor of user k in the context c.

M is the number of history ratings.

μ_{jkc} is the j^{th} optimistic nature of user k in the context c.

υ_{jkc} is the j^{th} pessimistic nature of user k in the context c.

This technique affects both the positive and the negative ratings of history due to which it is not sufficient to tackle with miss detection rate. Hence, in case of negative result, [0,M] may be added to the history. However as there is no need of punishing the user if the final decision is in the favor of PU, due to which [1,0] is added in case of positive rating, [0,1] is added in case of negative rating and [1,1] is added to the history of abstained user. However, if the SU base station itself is in confusion and final decision is zero then no reward is added.

IV. Simulation Result and Analysis

In this section, the robustness and efficiency of the proposed algorithm is evaluated. The model is simulated by considering 100 SUs and 8 PUs. A random variable is considered to decide the value of ϕ for each SUs and SU base station. The value of mean is considered as 0.5 whereas the value of variance is 0.25. Further, the confidence threshold of the node is considered as 0.25 and the node whose confidence threshold is less than 0.25 is not considered for sensing. The trust threshold Ω is set to 0.65 and the nodes whose value of trust factor is below the considered threshold are not considered by the SU base station for making final decision. Two forgetting factors ρ_1 and ρ_2 are considered as 1 and 0.9 respectively.

In order to calculate the effectiveness of proposed algorithm, Total Utility Loss(TUL) is defined as:

$$TUL = \varpi_1 \nu_1 + \varpi_2 \nu_2$$

where, ν_1 is the error rate produced by false alarm, ν_2 is the error rate produced by miss detection, ϖ_1 is the weight factor of ν_1 and ϖ_2 is weight factor of ν_2.

Since, miss detection errors are more severe and harmful as compared to the false alarm errors therefore, ϖ_2 is given more weightage than ϖ_1. Hence the values assigned to ϖ_1 and ϖ_2 is 1 and 10 respectively. Further, attacker ratio (σ) is taken into consideration and is defined as the number of malicious users present in the system.

The efficiency and the robustness of the proposed algorithm is checked by considering following attacks.

A. Fabrication Attack

When, SUs always provide false results i.e. opposite to the sensing results, then it is termed as fabrication attack. This attack either prevents the unlicensed users from accessing the spectrum or create excessive amount of interference to the licensed users. The final decision depends upon the number of spurious nodes present in the system. If the number of malicious nodes are in majority then the final decision is incorrect otherwise it is correct. It is considered that 50% of the total SUs are malicious with $\alpha = 50\%$. The error rate of the system is directly dependent on the spectrum usage by the licensed users. It has been observed that the proposed method is able to reduce the value of total utility loss with attacker's ratio greater than 40%. Therefore, it is concluded that the proposed algorithm shows robustness under fabrication attack.

B. True-False Attack

It is a dynamic strategy, in which the malicious users switch their opinions between correct and incorrect sensing results. The malicious users attain high reputation by providing correct sensing results and then use this reputation in order to deceive the system by sending incorrect sensing reports to the SU base station. Let t be the rate of true-false error. The case with $\sigma < 40\%$ is not considered as total utility loss tends to be 0 in that case. Whereas, total utility loss get diminished when the proposed method is adopted with attacker's ratio greater than40%. Figure 1 indicates the variation in total utility loss (Φ) under true-false attack.

C. Denial of Service attack

In this type of attack, the presence of PUs is always reported by the malicious nodes in its sensing report. It is indicative in figure 2 that the proposed algorithm performed well and total utility loss is inversely proportional to the spectrum band usage by the PUs. Further, total utility loss plot with attacker's ratio as 100% is not shown because it is unlikely that all the users account the presence of PU when actually it is not present.

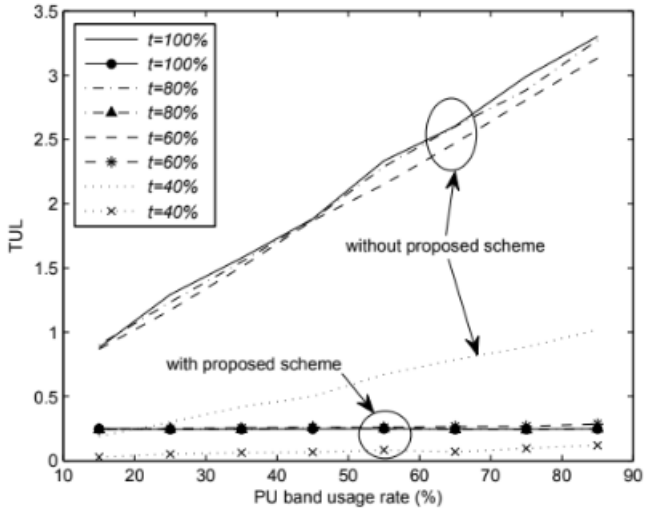

Fig. 1. Total utility loss under true-false attack with attacker's ratio $= 100\%$

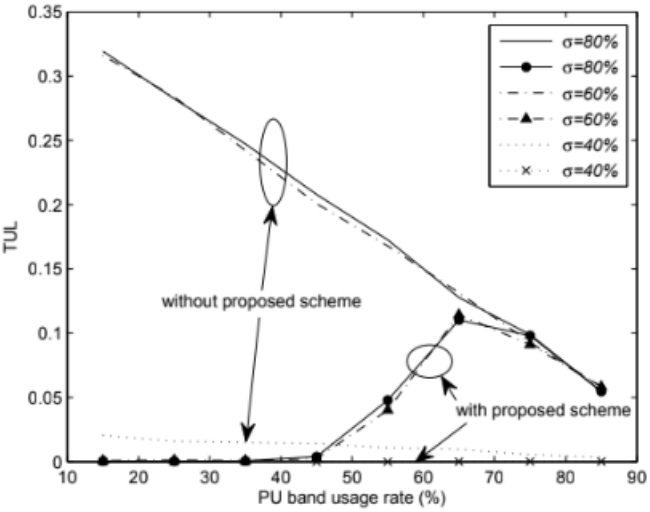

Fig. 2. Total utility loss under Denial of Service attack

Figure 3 represents the trust score attain by all the SUs when the usage rate of the spectrum band is considered as 45% and 75% respectively and it is concluded that trust score factor is dependent on the context.

D. Greedy Attack

In this type of attack, the spurious user always accounts the absence of PU to the SU base station. If the final decision is influenced by the sensing reports of the malicious nodes then PU face interference and SU base station gets punishment. The value of total utility loss of the CRN under the greedy attack is shown in Figure 4. Further, Figure 5 shows the filtering of these types of nodes.

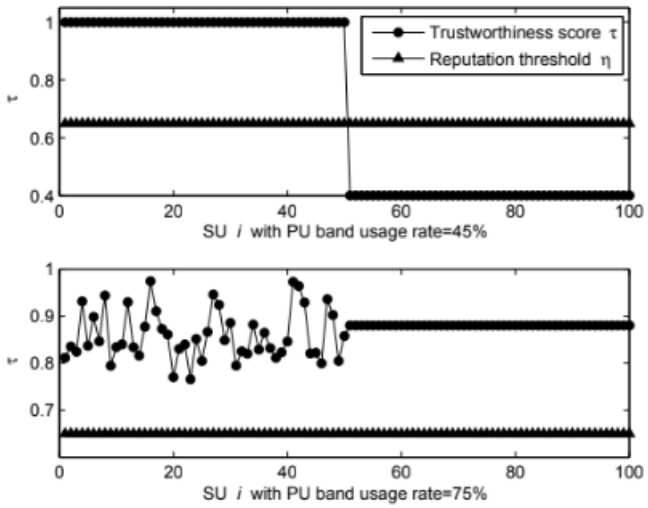

Fig. 3. Trust score t under Denial of service attack with attacker's ratio as 50%.

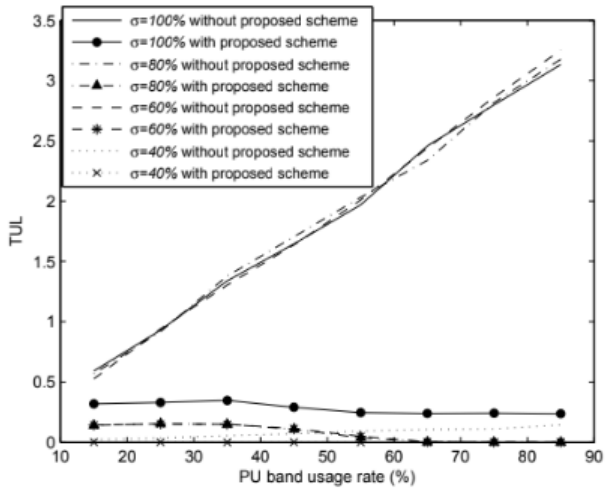

Fig. 4. Total utility loss under greedy attack.

E. Amalgamation of Attacks

It is highly probable that more than one attack is present in the system. Therefore, it is necessary to check whether the system is efficient and robust against different types of attacks collectively. The total utility loss under true false attack and denial of service attack collectively with trust score 20% and attacker's ratio as σ_1 and σ_2 respectively is shown in figure 6.

Further, the total utility loss under true false attack and greedy attack collectively with trust score 20% and attacker's ratio as σ_1 and σ_2 respectively is shown in figure 7

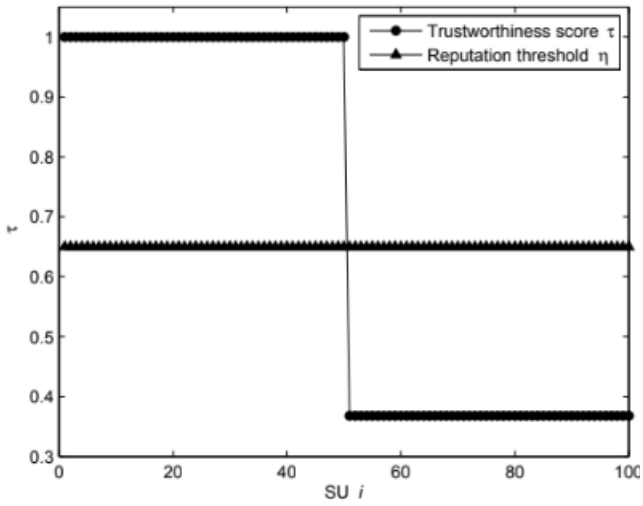

Fig. 5. Trust score t under greedy attack with attacker's ratio as 50%.

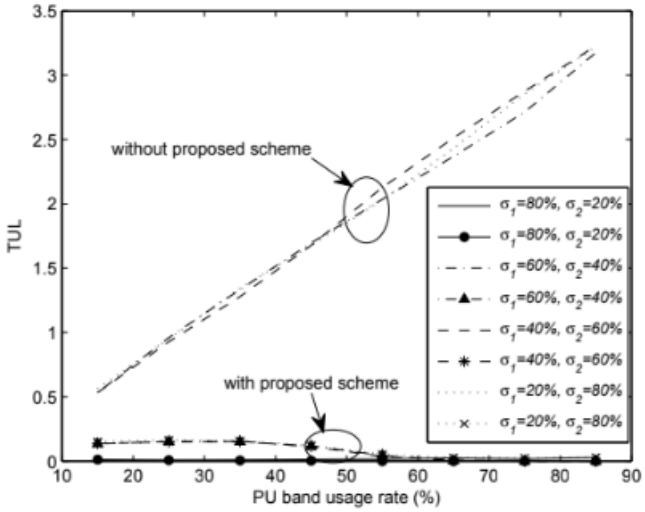

Fig. 7. Total utility loss under true-false and Greedy attack.

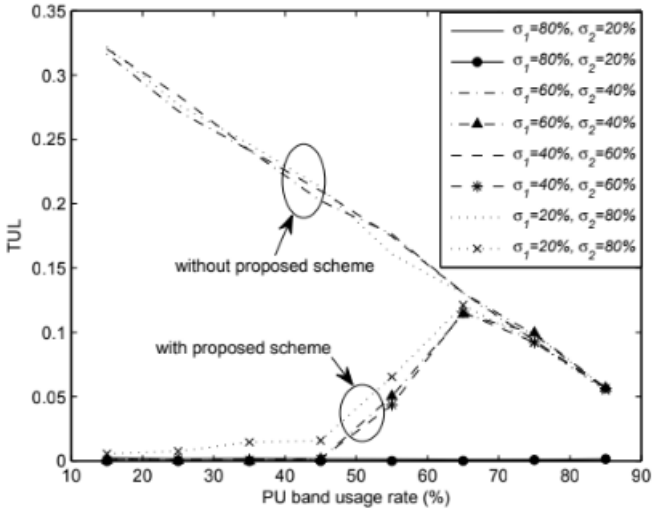

Fig. 6. Total utility loss under True-False and Denial of Service attack.

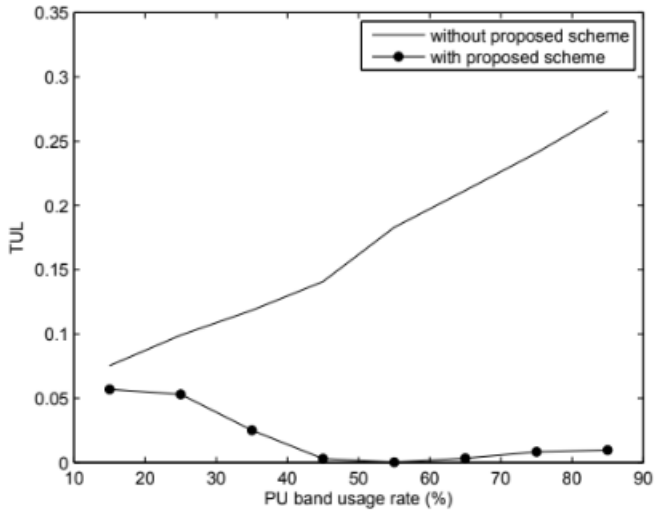

Fig. 8. Total utility loss under true-false, Greedy attack, fabrication and denial of service attack.

The total utility loss under true-false attack with trust score as 20% and attacker's ratio as 50%, greedy attack with attacker's ratio as 10%, fabrication attack with attacker's ratio as 30% and denial of service attack with attacker's ratio as 10% collectively is shown in figure 8. It can be concluded that all the attacks are handled effectively by the proposed algorithm.

Further, the trust value of each SU under true-false with attacker's ratio as 50% and attack rate as 20%, greedy attack with attacker's ratio as 10%, fabrication attack with attacker's ratio as 30% and denial of service attack with attacker's ratio as 10% is shown in figure 9.

V. Conclusion

There is a possibility of presence of the malicious nodes in the CRN. These malicious nodes may affect the final sensing results in cooperative spectrum sensing due to which efficiency of the CRN may get degraded. The proposed algorithm helps in finding the malicious nodes present in the network. In the present work, the algorithm find the malicious nodes by considering the trust value and filter out these nodes from the final decision. Further, performance evaluation of the proposed algorithm is performed in order to find the variation in total utility loss under the influence of various attacks. In

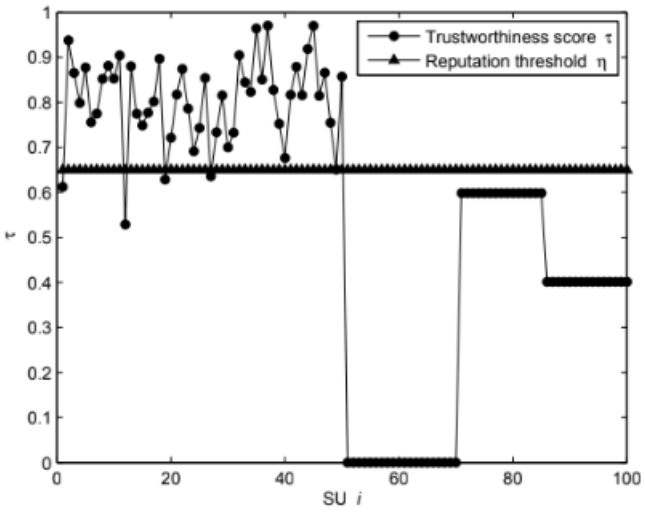

Fig. 9. Trust value of each SU under true-false, greedy attack, fabrication and denial of service attack.

future, various attacks can be studied where PU base station and SU base stations are not trustworthy. Further, performance of proposed scheme can be studied on ad-hoc , mesh and distributed systems.

REFERENCES

[1] N. Gupta, S. K. Dhurandher, and B. Kumar, "Cognitive radio networks: A comprehensive review," in *Handbook of Research on the IoT, Cloud Computing, and Wireless Network Optimization*. IGI Global, 2019, pp. 491–518.

[2] N. Gupta and S. K. Dhurandher, "Cross-layer perspective for channel assignment in cognitive radio networks: A survey," *International Journal of Communication Systems*, p. e4261, 2019.

[3] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical communication*, vol. 4, no. 1, pp. 40–62, 2011.

[4] N. Gupta, S. K. Dhurandher, and A. Sehgal, "A contract theory approach-based scheme to encourage secondary users for cooperative sensing in cognitive radio networks," *IEEE Systems Journal*, 2019.

[5] S. A. V. Yazdi and M. Ghazvini, "Countermeasure with primary user emulation attack in cognitive radio networks," *Wireless Personal Communications*, pp. 1–17, 2019.

[6] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[7] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691–1708, 2012.

[8] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2012.

[9] I. A. Sohu, A. A. Rahimoon, A. A. Junejo, A. A. Sohu, and S. H. Junejo, "Analogous study of security threats in cognitive radio," in *2nd IEEE International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, 2019, pp. 1–4.

[10] S. Mapunya and M. Velempini, "Investigating spectrum sensing security threats in cognitive radio networks," in *Ad Hoc Networks*. Springer, 2018, pp. 60–68.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *2009 43rd Annual Conference on Information Sciences and Systems*. IEEE, 2009, pp. 130–134.

[12] E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system," in *2010 IEEE 71st Vehicular Technology Conference*, 2010, pp. 1–5.

[13] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in *IEEE Global Telecommunications Conference (IEEE Globecom)*, 2009, pp. 1–6.

[14] T. Bansal, B. Chen, and P. Sinha, "Fastprobe: Malicious user detection in cognitive radio networks through active transmissions," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, 2014, pp. 2517–2525.

[15] A. A. Sharifi, "Attack-aware defense strategy: A robust cooperative spectrum sensing in cognitive radio sensor networks," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, no. 1, pp. 133–140, 2019.

[16] X. Huang, N. Han, G. Zheng, S. Sohn, and J. Kim, "Weighted-collaborative spectrum sensing in cognitive radio," in *2007 Second International Conference on Communications and Networking in China*. IEEE, 2007, pp. 110–114.

[17] M. Matsui, H. Shiba, K. Akabane, and K. Uehara, "A novel cooperative sensing technique for cognitive radio," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007, pp. 1–5.

[18] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun, "Cognitive radio network architecture: part ii–trusted network layer structure," in *Proceedings of the 2nd international conference on Ubiquitous information management and communication*. ACM, 2008, pp. 120–124.

[19] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*. IEEE, 2008, pp. 1–8.

[20] S. Kar, S. Sethi, and R. K. Sahoo, "A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks," *Wireless Personal Communications*, vol. 97, no. 2, pp. 2523–2540, 2017.

[21] S. K. Dhurandher, I. Woungang, N. Gupta, R. Jain, D. Singhal, J. Agarwal, and M. S. Obaidat, "Optimal secondary users selection for cooperative spectrum sensing in cognitive radio networks," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–6.