A Study on Techniques/Algorithms used for Detection and Prevention of Security Attacks in Cognitive Radio Networks

SUDHA Y
Assistant Professor, Department of Computer Science and Engineering, Presidency University,Bengaluru

Abstract- **In this paper a detailed survey is carried out on the taxonomy of Security Issues, Advances on Security Threats and Countermeasures ,A Cross-Layer Attack, Security Status and Challenges for Cognitive Radio Networks, also a detailed survey on several Algorithms/Techniques used to detect and prevent SSDF(Spectrum Sensing Data Falsification) attack a type of DOS (Denial of Service) attack and several other Network layer attacks in Cognitive Radio Network or Cognitive Radio Wireless Sensor Node Networks(WSNN's) to analyze the advantages and disadvantages of those existing algorithms/techniques.**

Keywords: **Cognitive Radio Networks (CRN); SSDF;DOS;WRSNN's; Cognitive Radio Wireless Sensor Node Networks (CRWSNN's);**

I. INTRODUCTION

A detailed survey has been carried out to identify the various research articles available in the literature on security issues, link layer attacks such as SSDF,DOS and several network layer attacks in Cognitive Radio Networks/CRWSNN's.Following are the literatures used for the assessment and analysis of the state-of-art work on the techniques /Algorithms used in CRN (cognitive radio networks) for attacks/threats detections and preventions.

Study of Security threats in Cognitive Radio Networks

Defensive Mechanism in Cognitive Networks

The study incorporate a security mechanisms by designing the monitoring framework (Spec Monitor) to monitor the system and detect malicious and abnormal behaviors in Cognitive Radio Networks. The security development techniques such as spectrum sensing in the cognitive network and non-parametric passive traffic monitoring in cognitive systems were evaluated and a detailed methodology is proposed to overcome the increasing complexity threats in Cognitive networks. Efficient and effective security monitoring mechanisms were also designed to defend the cognitive network against sophisticated attackers that exploit vulnerabilities of CRNs. The non-parametric passive traffic monitoring was also evaluated as the core technique used to protect the cognitive network from security threats. The methods for the calculation of safety loopholes were also identified together with other system defending mechanisms. The evaluation incorporated mathematical formula, prototypes, and tested techniques.

Major Security Threats within a Cognitive Radio Network (CRN) framework.

A comprehensive list of major known security threats within a cognitive radio network (CRN) framework is listed in this section. The attacktechniques were classified based on the type of attacker, namely exogenous (external) attackers, intruding malicious nodes and greedy cognitive radios (CRs). It further discuss threats related to infrastructure-based CRNs as well as infrastructure-less networks. Besides the short-term effects of attacks over CRN performance, the authors also discuss the often ignored longer term behavioral changes that are en- forced by such attacks via the learning capability of CRN. After elaborating on various attack strategies, apotential solutions to combat those attacks were also discussed. An overview of robust CR communications is also presented.an array of solutions, mainly based on trust ranking of cooperating nodes, have been developed to combat SSDF attacks.

A Survey of Security Issues in Cognitive Radio Networks

Thispaper, considers the security threats from passive and active attacks. Firstly, the PHY layer security is presented and in the view of passive attacks using the physical properties of the radio channel to help provide secure wireless communications. Moreover, malicious user detection is introduced in the view of active attacks by means of the signal detection techniques to decrease the interference and the probabilities of false alarm and missed detection. Finally, the section discuss the general countermeasures of security threats in three phases. In particular, the authors discuss the far reaching effect of defensive strategy against attacks in CRNs.

this article have analyzed the security issues in cognitive radio networks and investigated the most important contributions on security threats and the current state of the art techniques. Firstly, it spots the security issues and provided a classifications of attacks in the CRNs. Secondly, A survey on the existing countermeasures for defensing against the active attacks. Thirdly, it present the PHY layer security in the view-point of passive attacks.

Recent Advances on Security Threats and Countermeasures

The main goalhere, is to present the state-of-the-art research results and approaches proposed for CRN security to protect both unlicensed secondary users and licensed primary users. Specifically, the recent advances on security threats/attacks and countermeasures in CRNs focusing more on the physical layer by categorizing them in terms of their types, their existence in the CR cycle, network protocol layers (exploited during their activities and defense strategies), and game theoretic approaches. The recent important attacks and countermeasures in CRNs are also summarized.The article also present recommendations that can be followed while implementing countermeasures to enhance CRN security.For CRN security, authors have presented the major threats in general and threats specific to different layers (including cross layers) of OSI reference models. The types of game theoretic models for CRN security has been reviewed. a side-by-side comparison summary is presented in a tabular form for different PUE attacks, SSDF attacks, eavesdropping attacks and attacks during both SU communication phase and sensing phase and their defense measures. Due to dynamic spectrum agility and opportunistic spectrum access for unlicensed users, CRN introduce entirely new classes of security threats and challenges. Wherever opportunistic spectrum access in wireless networks is deployed, security attacks and vulnerability will always exist. There will be no single method that can secure the entire cognitive wireless networks. To handle variety of security attacks and threats, implementation of combination of countermeasures and context- based machine learning techniques would be needed to protect future wireless systems.

Comparative study of Security threats

This study focuses on security issues which are related to CRWSN as Fusion techniques, Co-operative Spectrum sensing along with two dangerous attacks in CR: Primary User Emulation (PUE) and Spectrum Sensing Data Falsification (SSDF). This paper discuss about dangerous attacks like PUE and SSDF. Also discuss about some frequent attack in cognitive radio CR. Threat detection and protection of data are severe issue in cognitive radio and also in wireless network.

II. A SURVEY ON SSDF (Spectrum Sensing Data Falsification) ATTACKS

Defensive technique for SSDF attack

This paper, provides a comprehensive survey and tutorial on the recent advances in the Byzantine attack and defense for CSS in CRNs. Specifically, firstly, present the preliminaries of CSS for general readers, including signal detection techniques, hypothesis testing, and data fusion. Secondly, propose a taxonomy of the existing Byzantine attack behaviors and elaborate on the corresponding attack parameters, which determine where, who, how, and when to launch attacks. Then, from the perspectives of homogeneous or heterogeneous scenarios, the existing defense algorithms are classified and provides an in-depth tutorial on the state-of-the-art Byzantine defense schemes, commonly known as robust or secure CSS in the literature. Furthermore, analyze the spear-and-shield relation between Byzantine attack and defense from an interactive game-theoretical perspective. Notably, the spear-and shield relation between Byzantine attack and defense was analyzed.

Clustering Algorithm to Counter SSDF attack

Here a comparative clustering algorithm is used for sensing data to counter the SSDF attack. The algorithm does not assume any information about the attacker. An accuracy graph is plotted according to the detection of the malicious users. If we come to complexity then the complexity of our algorithm turns out to be O (N*m*no. of iterations) whereas the algorithm turns out to be O(NM) which is much larger than the complexity of the algorithm.

Attack-Aware Collaborative Spectrum Sensing Approach

A new defense scheme called attack-aware CSS (ACSS)is proposed here. The proposed method estimates attack strength and applies it in the k−out−N rule to obtain the optimum value of k that minimizes the Bayes risk. The attack strength is defined as the ratio of the number of malicious users to the total number of users, which is equal to the probability that a specific user is malicious. The obtained results verified that the proposed approach is a robust defense method against SSDF attacks.

K-Medoids Clustering to Mitigating SSDF Attack

In infrastructure-based cognitive radio network, each node sends its local sensing report to the fusion center which uses a fusion rule to make the final decision. The decision of the Fusion Center plays a vital role. Attackers may try to manipulate the decision-making of the Fusion Center (FC) for selfish reasons or to interfere with the primary user transmission. In SSDF attack, malicious users try to manipulate the FC by sending false sensing report. this paper presents a method for detection and isolation of such malicious users. This method is based on the k-medoids clustering algorithm. The proposed approach does not require the use of any predefined threshold for detection. It mines the collection of sensing reports at the FC for determining the presence of attackers. Additionally, the proposed approach can be used on streaming data (sensing reports) and thereby detect and isolate attackers on the fly. Simulation results support the validity of the approach.

Joint spectrum sensing and resource allocation (JSSRA) scheme in CRN

Spectrum sensing and spectrum sharing are two fundamental issues in a cognitive radio network (CRN). The spectrum sensing data falsification (SSDF) attack imposes bad effects on both spectrum sensing and spectrum sharing. To deal with SSDF attacks and to incentivize secondary users (SUs) to behave well, a joint spectrum sensing and resource allocation (JSSRA) scheme in a CRN is proposed in this paper. The JSSRA problem is formulated as a weighted-proportional-fairness-based resource-allocation optimization problem under the constraint that the primary user (PU) network is sufficiently protected. The problem is decomposed into two sub-problems, namely, the resource allocation sub-problem and cooperative SU number decision sub-problem, which are solved by the Lagrangian dual algorithm and the brute– force algorithm, respectively. Moreover, a user-selection method based on reinforcement learning is presented to select reliable SUs for cooperative spectrum sensing (CSS). In addition, the SU’s trust degree is updated according to its behavior in CSS and is used in the sensed resource-allocation process. The key point of the proposed scheme is to make SUs improve the sensing reliability and prevent SUs from behaving maliciously by an incentive mechanism. Comprehensive performance evaluation is conducted by computer simulation. It is shown that the proposed JSSRA scheme deals with the SSDF attack well in cooperative sensing process to improve system robustness and achieves a significant system utility gain in resource allocation. This paper proposed the JSSRA scheme for the CRN with SSDF attack. The proposed scheme consists of five modules, namely, the JSSRA optimization, cooperative user selection, CSS, resource access, and SU’s trust degree and learning parameter update.

Association Rule Mining detection technique Colluding SSDF Attack

A detection schemeis based on Apriori algorithm is used to detect colluding SSDF attack. The validity of the proposed scheme is supported through extensive simulation results. Colluding SSDF attacks have been found to degrade performance more than independent SSDF attacks.

Trust-based Cooperative Spectrum Sensing technique against SSDF Attacks

A trust-based data fusion scheme against spectrum sensing data falsification attacks in a distributed cognitive radio network is proposed and analyzed.The trust-based data fusion scheme is based on mechanism design theory to motivate users to report authentic sensing data so as to improve the success rate. Further, we decouple erroneous sensing reports due to low sensing capabilities from false reports due to attacks, thus avoiding unnecessary punishments to benign users. A theoretical analysis have been conducted to validated with extensive simulation and identify optimal parameter settings under which our trust-based data fusion scheme outperforms existing non-trust based data fusion schemes.

Assessment of Simultaneous Multiple DOS attack in CRN

One main challenge in CR network security domain is to efficiently represent possible simultaneous multiple security threats, and assess their effects. Unlike the previous works, this paper addresses the combined effect of simultaneous multiple DoS attacks through using the holistic approach.The Bayesian Attack Graph (BAG) model is utilized in this paper to capture the probabilistic dependencies among IEEE 802.22 DoS threat–environment and known vulnerabilities. The simulation results indicate up to 51.3% increase in the probability of DoS in IEEE 802.22 networks considering simultaneous multiple attacks in comparison to the most severe sole attack. Finally, the paper introduces the BAG model as a feasible CR vulnerability metric that can facilitate the creation of a security tightening plan.

Secure Collaborative Spectrum Sensing: A Peer-Prediction Method

Collaborative spectrum sensing is an effective method to improve detection rates in cognitive radio networks. However, it is vulnerable to spectrum sensing data falsification (SSDF) attacks when malicious secondary users (SUs) report fraudulent sensing data. An incentive method based on peer-prediction is proposed to identify malicious suspects, punish attackers, and incentivize SUs to send truthful reports simultaneously for decision fusion. Moreover, continuous peer-prediction derived from the binary case is introduced, which is capable of preventing attacks in the continuous domain. Theoretical analysis and simulation results demonstrate that honest SUs are rewarded for accurate and truthful sensing results, while malicious SUs incur penalty for making falsified sensing reports. A significant improvement of detection rates is obtained by the proposed scheme when there are no more than half of malicious SUs conducting SSDF attacks. Here two incentive attack prevention schemes are proposed , for collaborative spectrum sensing in CRNs based on decision fusion and data fusion to motivate SUs to report truthful sensing results and identify malicious suspects based on private-prior peer-prediction and continuous private- prior peer-prediction.

Soft Fusion-defense technique Against SSDF Attacks.

This paper mainly study the CSS based on soft-fusion, in order to defend against the SSDF attacks launched by MUs and guarantee the detection performance of the system as far as possible, based on the traditional EGC soft fusion algorithm we make improvements that regard the cooperation as a service-evaluation process and make use of CUs' average reputation degrees to reflect the service quality, then allocate properly the CUs' weights in the fusion according to the reputation degrees instead of the equal weights allocation. Through simulation and comparing with EGC algorithm, the effectiveness of the improved soft fusion algorithm against SSDF attacks is verified.

A Simple and Highly Effective SSDF attacks Mitigation Method

This paper presents a method to alleviate spectrum sensing data falsification (SSDF) attacks in cognitive radio networks. A reputation based scheme is used here to mitigate the effects that shadowing and noise have on local observations. The method presented in this paper is a simple, highly effective way to mitigate spectrum sensing data falsification attacks. It is able to converge quickly and offers high accuracy identification and mitigation of a malicious node. The proposed method is based on a modified belief propagation algorithm that uses reputation as a weighting factor.The simulations verify that the algorithm enables effective distributed spectrum sensing even with substantial SSDF attacks.

Defense Mechanism to Mitigate the Spectrum Sensing Data Falsification attack in Cognitive Radio Ad Hoc Networks

This section presents the integration of two infrastructure-based schemes to mitigate the effects of the SSDF attack in infrastructure-less topology, the reputation and q-out-of-m rule schemes. The reputation scheme is used to isolate outliers before the final transmission decision is made and the q-out-of-m rule scheme is used to protect the network from nodes that are able to change their reports to avoid being regarded as outliers. This scheme is implemented in CRAHN where the presence of a data fusion centre is not required. The scheme was evaluated analytically. Future work will evaluate the scheme numerically.

Neighbor Detection-Based Spectrum Sensing Algorithm

To defense against (SSDF) attack, a neighbor detection-based spectrum sensing algorithm is proposed in distributed CRNs, which can detect attackers with the help of neighbors during spectrum sensing to improve the accuracy of decision making. The proposed scheme can also guarantee the connectivity of the network. thealgorithm can remove suspicious nodes according to their data variation and adjust trust neighbor nodes set when the set is changed to maintain the connectivity. Simulation results illustrate that the proposed scheme can defense against SSDF attacks effectively and reach the unified information of spectrum sensing data. The algorithm can not only make CRNs robust against different kinds of SSDF attacks, but also achieve a unified sensing result more quickly.

Novel attack-proof CSS scheme with M-ary quantized data

This scheme, addresses the challenging and important cooperative spectrum sensing (CSS) problem with M-ary quantized data under spectrum sensing data falsification (SSDF) attacks. a probabilistic SSDF attack model is introduced to characterize the attacks by a malicious secondary user (SU). the attack behavior is analyzed and derive the condition to nullify the detection capability of the fusion center (FC). To defend against the SSDF attacks, a novel attack-proof CSS scheme is proposed with M-ary quantized data, mainly including a malicious SU identification method and an adaptive linear combination rule. By using the malicious SU identification approach, FC identifies malicious SUs and removes them from the data fusion process. The adaptive linear combination rule adjusts the weighted coefficients with the distribution parameter sets of identified normal SUs estimated using a maximum likelihood- based estimator. FC performs the spectrum sensing process with M-ary quantized data from the identified normal SUs. Comprehensive evaluation is conducted. Evaluation results show that the proposed malicious SU identification method can remove malicious SUs successfully and the proposed CSS scheme is robust against the SSDF attacks.

An Effective Collaborative Spectrum Sensing Method against SSDF Attack

An effective Correlation coefficient method is used here against Byzantine attack (also known as SSDF attack) for collaborative spectrum sensing problem. Firstly, the proposed method exploits the path loss factor to improve the reliability of the data. And then, the fusion center utilizes the correlation of the perceived data in different time windows to detect the attackers. Eventually, the fusion center makes the final decision by comparing the detection statistics and the threshold weighted with path loss factor. Simulation results testify the effectiveness of the presented algorithm. The simulation results show that the proposed algorithm can not only reduce the influence of path loss on detection performance, but also can restrain the attack behavior of malicious users.

Fast reputation-based algorithm/ Reliable Spectrum Sensing (RSS) to defeat SSDF attack.

This proposed scheme employs an efficient and fast reputation-based algorithm to analyze the behavior of each user. Hence, not only will reliable sensory data be accepted by the central entity, but also, malicious users can be easily identified and removed from the network. Both theoretical and simulation results show that the proposed method provides a powerful countermeasure against SSDF attacks in an adversarial CR environment. In this article, a new defense scheme called Reliable Spectrum Sensing (RSS) is presented. The proposed method mitigates the harmful effect of malicious CR nodes on the performance of CSS in the presence of SSDF attackers. RSS adopts location-based credentials, hence the effect of the compromising nodes is limited to its vicinity. The proposed scheme is evaluated and extensively analyzed. The obtained results attest that RSS is a robust defense strategy to countermeasure SSDF attacks and successfully reduce its effect on the system.

Optimal reputation-based detection scheme for industrial cognitive radio networks (ICRNs).

To address the issues of SSDF attack in industrial cognitive radio networks (ICRNs) an optimal reputation-based detection scheme is proposed with considerations of the attack probability. Moreover, the threshold of reputation value is specially designed to adapt to the varying attack probability which can be estimated by past performance. To estimate the attack probability, the maximum likelihood estimation method is used in certain CSS rounds. Numerical results reveal that the proposed detection scheme performs better than existing reputation-based detection schemes.

Bayesian online/offline learning defense against SSDF attack

In this paper, Bayesian learning is used to design Byzantine defense schemes. First, a Bayesian offline learning algorithm is developed by considering one practical challenge that the ground-truth spectrum state is unavailable for training. Then, a Bayesian online learning algorithm is developed by considering the case that the sensors' attribute may be time-varying. The first contribution was to introduce the Byzantine offline learning to train the historical spectrum sensing data. The second contribution was to propose a attacker-identification algorithm, based on Bayesian online learning, that is able to detect attackers and eliminate their influence on CSS. In addition, a simulations is presented to show the performance of the proposed defense algorithms.

Credit Threshold scheme for Mobile Cognitive Radio Networks

In this paper, uses a two-stage credit threshold (TSCT) scheme based CSS to counter arbitrary number of MUs who exist in CRNs. the network region is divided into cells according to channel condition, and CSS procedure is conducted into two stages, which are the secondary user (SU) stage and cell stage. The proposed scheme can effectively remove MUs in the SU stage and weaken the bad effects of remnant MUs in the cell stage. In comparison to existing schemes, simulation results show that the proposed scheme can provide with better detection performance regardless of detection rounds, and can work well when MUs outnumber SUs while previous schemes fail.

Self-Organizing Map-Based Scheme against SSDF attack.

To deal with SSDF attack, one of the typical artificial neural networks (ANN): self-organizing map (SOM) neural network is recommended. SOM network possesses the ability of classifying the SUs into categories with different frequency of occurrence. Exploiting this characteristic, an algorithm calculating the suspicion degree (SD) of each SU is proposed. Considering that SD can't maintain the stability of classification results, we further propose the concept of average suspicion degree (ASD) and readjust the weights of SUs according to their ASD. Simulation results reveal that compared with the results of traditional SOM algorithm and dynamic threshold algorithm, the detection performance of our method shows improvement. In a word, SOM algorithm possesses great potential against SSDF attack in CRN in the future.

GLRT and Eigen value Based Method for CR.

This methods investigate the performance matrices of cognitive radio technology under Energy detection and Eigen value based detection technique. Under Eigen value based detection technique, we consider GLRT (Generalized likelihood ratio test) and maximum and minimum Eigen value based methods for decision threshold calculation. Threshold in Eigen value detection technique defined on the basis of Random matrix theory. Eigen value based technique performs better then energy detection based technique under noise uncertainty.

The message authentication code (MAC) technique.

The message authentication code (MAC) is a promising technique to avoid the damage from the spectrum sensing data falsification (SSDF) attacks. An proposed energy efficiency model to capture the effects of the length of MAC and the number of cooperative SUs under independent and collaborative SSDF attacks, respectively, and analyze the existence of the optimal length of MAC and the optimal number of cooperative SUs that can achieve the maximum value of energy efficiency, respectively. Simulation results are provided to show that the CSS scheme based on MAC can resist SSDF attacks and the accuracy of the theoretical analysis is also validated.

Robust Cooperative Spectrum Sensing model against SSDF attack

This paper, investigates the problem of cooperative spectrum sensing in CRNs in the presence of SSDF attack by developing a general SSDF attack model and proposes a robust data fusion scheme, named robust weighted sequential probability ratio test (RWSPRT), which can deal with various attack probabilities. In the proposed RWSPRT, according to the correct decision ability, the reputation value (RV) of each SU is integrated into weight coefficient of weighted sequential probability ratio test (WSPRT) to improve the performance of cooperative spectrum sensing. Simulation results show that RWSPRT performs more robust than traditional data fusion techniques whereas requires less number of samples, even when a large number of MUs exists in CRNs.

Evidence-theory-based secure sensing approaches in CR.

Here In order to defense against malicious SSDF attacks, certain evidence-theory-based secure sensing approaches have been proposed. However, in most of the current evidence-theory-based CSS schemes, only real- time evidence information is utilized to estimate the sensing reliability of cognitive users, like the difference in SNR or similarity degree. Inadequate consideration causes CSS system being vulner- able to SSDF attacks, and the correctness of global decision making cannot be guaranteed. this paper, proposes a credible CSS scheme based on evidence theory. It evaluates the credibility of each SU with two indexes, which are the statistical reputation factor and the real-time reliability factor, respectively. In addition, considering the transmitted data rises with the number of SUs increasing, we propose a rational mass distribution (RMD) approach to adjust evidence theory to binary hypothesis test in spectrum sensing context. As a consequence, both the data volume to be transmitted and the workload at data fusion center has been reduced. Simulation results have proved that the proposed scheme is effective and robust to defense against distinctive SSDF attack patterns.

Dynamic trust mechanism based on Beta reputation system against SSDF attacks

In this article, a dynamic trust mechanism based on Beta reputation system is proposed to resist SSDF attacks. This method introduce the time proportion coefficient, which is set in line with the historical sensing behaviors of cognitive users, and the reputation value of users can be obtained accordingly, besides, the rise factor and fall factor are introduced as well. Cognitive users that are qualified to participate in the cooperative sensing can be selected in accordance with users' reputation values. The final global decision can be obtained by linear fusion method in the center data fusion. Simulation results show that, in the proposed reputation mechanism, the SSDF attack is effectively suppressed since the reputation of malicious cognitive users are significantly reduced, thus improving the accuracy of cooperative spectrum sensing.

Angle based Malicious User Detection for Wideband Cognitive Radio Network

In this paper, the attack and defense behavior in wideband CRN is studied as well as proposed an angle based malicious user detection (ABMUD) algorithm for wide- band cooperative CRN, in which an ABOD based linear approximation approach (noted as FastABOD method) with adaptive decision mechanism is used to recognize independent malicious users. The simulation results show that the performance of the proposed ABMUD algorithm has a greater improvement, compared to the traditional DSND algorithm for the small-scale SSDF independent attack detection.

Fuzzy Clustering Means (FCM) algorithm

Fuzzy Clustering means (FCM) are proposed here to mitigate the malicious user behavior than heretofore existing methods. The proposed approach improves the packet delivery ratio much larger than the preceding methods. The result has been taken in the time of packet transfer from one node to another node. The proposed research has been simulated in the Network Simulator software of Version 3. Robustness of this approach was favored by simulation results. In the existing ones, mitigation of SSDF attack was done by using the Multi-factor Trust Management Scheme. This will assess the trustworthiness of every node, which takes part in Cooperative spectrum sensing. The proposed scheme gives good performance in de-centralized Network. The same operation will be taken place in each sensor nodes of SU’s. Several methods are used to fulfil the attack prevention, but FCM methods are not used up to now to mitigate Spectrum sensing data falsification Attack. This shows better performance than the existing method.

Secure Non-Consensus Based Spectrum Sensing in Non-Centralized Cognitive Radio Networks

In this section, a non-consensus based distributed spectrum sensing (NCSS) scheme is presented, in which a node uses the raw energy level of the PU signal from its h-hop neighbors for determining the status of the PU. A message passing scheme is used rather than the conventional consensus scheme. A comparison with an existing consensus algorithm is also shown. Further, two types of spectrum sensing data falsification attacks are considered in which the attackers inject very high or very low energy values. To catch such abnormal behavior of a node, an approach called secure NCSS algorithm is proposed, which isolates a node that generates extreme energy values so that it is removed from future computation. For this, an outlier detection technique is adopted. The approach is based on the idea that a malicious node’s energy level deviates significantly from those of genuine nodes, whereas all genuine nodes share nearby estimated energy levels.

Lightweight cloned-node detection algorithm to handle SSDF attacks

Cognitive Wireless Sensor Networks (CWSNs) provide better bandwidth utilization when compared with normal wireless sensor networks. CWSNs use a technique called opportunistic spectrum access for data transfer. In the node cloning attack, the malicious node creates many clones of the compromised node in the network. In order to confuse the collaborative spectrum sensing system, the clone nodes can send false spectrum sensing reports in a large number. The maximum-match filtering (MMF) algorithm is used for making a secure spectrum sensing decision in CWSNs. The Cloned-Node Detection (CND) algorithm is proposed here to detect cloned nodes. This study also explains how the CND algorithm based on Cuckoo hashing technique assists the MMF algorithm to make better spectrum sensing decisions by avoiding the node cloning attack. The algorithm is space efficient and has a low false-positive rate for a large network. We have also explained the MMF algorithm. This algorithm compares the similarity of sensing data and to plots those similar values in a three-dimensional space. It draws a regression plane on those plotted values and considers only those sensing results for spectrum decision whose similarity values lie on the regression plane to counter the SSDF attack. Further, we have explained the effect of the node cloning attack on the majority voting-based system. Our algorithm produced good results with relatively small data sets. An accuracy graph is plotted according to the detection of the malicious users.

Trust based defensive method against SSDF attacks

The reputation-based system was used to determine the trustworthiness of the SUs by evaluating their past reports. Reports with reputation values above the selected threshold value were discarded from the decision making process and were deemed as malicious reports. Reports below the threshold value were selected for decision making. After the final transmission was made, the SUs with reports different from the final transmission decision reputation values were incremented by 0.1. This paper implemented the reputation- based system with a threshold value of 0.6 to accommodate the MSU but also to preserve the integrity of CRN. The scheme is implemented in Mat lab simulation tool installed in Windows 10 operating system. The probability of false alarm, missed detection and the success probability were used to test the effectiveness of the proposed scheme.

Greedy Method in Dense Cognitive Radio Networks

This paper presents a method for detecting a set of spectrum sensing data falsification (SSDF) attacks, in a geographic database (GDB) enabled cognitive radio (CR) system. Viewing the GDB as a type of non-orthogonal CS dictionary, the composite power spectral density (PSD) estimate at a candidate user is approximated by a small number of sensor nodes listed in the GDB. In a dense CR network, the PSD estimate at a CR may contain a mixture of spectrally overlapping signals. An implementation of the greedy algorithm orthogonal matching pursuit (OMP) is proposed to return a set of sensor nodes which are suspected to be in the vicinity of the CR. A sufficient match between the PSD estimate reported by a candidate user and the PSD that is sparsely approximated from the SNs in its area provides a confidence/trust metric, which can be used to detect potential SSDF attacks. Specific SSDF attacks are reviewed and some recent methods in optimal sensing matrix construction for CS using an overcomplete dictionary are applied to address some of the key operational challenges in this scenario. Simulations provide insight into the detection performance and show that the specified SSDF attacks can be detected amidst additive white Gaussian noise and dictionary mismatches. Benefits of the proposed method include the ability to roughly localize a spoofing SU within the CRN by correlating the received spectrum report with the entire GDB and the ability to detect spectrum inversion by analyzing the sign of correlation. SA-OPT provides greater SN matching in the presence of heavy channel re-use throughout the CA and dictionary miss-matches brought on by SUs blocked by terrain or other obstructions.

Secure fusion strategy which adopts “soft decision” method

Essentially, all existing representative schemes utilize certain low- dimensional human-observed metric to distinguish malicious users and honest users based on domain knowledge. Therefore, these defense mechanisms cannot perform properly under certain condition, such as sensing reports with different distributions but have equal mean and variance This paper proposed a maximum mean discrepancy (MMD)based secure fusion strategy to defend against intelligent SSDF attack for collaborative spectrum sensing in CRNs. the proposed scheme is suitable for general CRN application scenarios wherein the PU can be any device (not limited to TV sets) operating on various spectrum bands (e.g. TVWS, SHF, EHF band). The fusion strategy makes full use of information from all users including both the honest users and malicious users. Unlike existing defense mechanisms that utilize low-dimensional metric determined by expert observations, this method can capture high-dimensional features of spectrum sensing data. Numerical results reflect the effects of different kernel functions and window size on the system performance, and show our scheme outperforms other existing approaches. The communication channels between SUs and the fusion center are assumed to be error-free in this paper

Performance Investigation of Insistent Spectrum Sensing Data Falsification on Cognitive Radio Networks

A cognitive radio ad-hoc networks, subordinates user must correlate decentralized way to discover the presence or non-presence of the main user. In such a setting, the malicious nodes are degenerates the correlate spectrum sensing performance by sending the inaccurate sensing information to the other nodes. We explore and contrast the affectability of these classes with range detecting information adulteration attacks and examine the advantage of confide in administration in im1proving the execution of these techniques. At the end, insistent spectrum sensing data falsification (ISSDF) attacks on iterative disseminated agreeable spectrum sensing. simulation outcomes display that the innovation techniques importantly enhance the cooperative sensing performance in the presence of malicious nodes in the network.

III. STUDY ON NETWORK LAYER ATTACKS

Security Techniques for Wormhole Attack

In this paper a structured literature for different types of attacks has been proposed. It presents worms attacks. Latest network security technologies are investigated, the current situation and increasing demand for robust network security is analyzed. Worms is one of the most common propagation attacks over the internet. Worm to propagate it can use two methods: finding any vulnerable devices in the network and propagate using topological neighbors. Worm’s propagation mechanism has been investigated and description about how it has evolved with the proliferation of data Transmission, instant messages and other communication Technologies has been described. The main worm propagation topology, scan-based techniques &topology-based techniques are described and investigated. A detailed methodology is proposed to overcome worm attack mechanisms. Based on which different attributes of information security have been analyzed which includes integrity, confidentiality, availability, authentication, non- repudiation and access control.

Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact

Cognitive Radio Ad Hoc Networks (CRAHNs) is the use of CR technology in the wireless ad-hoc network scenario. this paper presents an implementation and simulation study of Network Layer Attacks primarily Black Hole Attack and Gray Hole Attack in detail with their impacts on the various network parameters. In this research work,using NS2 with the CRAHN extension as the simulator, effect of these attacks on the various network parameters of CRAHNs have been recorded and compared to present an oversight of how performance is affected whenever the network gets injected with these attacks. After deep analysis, it was concluded that the characteristics of the results obtained for Gray Hole attacks were the same as the Black Hole Attack but their impact was comparatively less severe thus proving that Black Hole Attacks are more dangerous than Gray Hole Attacks.

HCOBASAA: Countermeasure against Sinkhole Attacks in Software-Defined Wireless Sensor Cognitive Radio Network

Network Software-defined wireless sensor cognitive radio network is one of the emerging technologies which is simple, agile, and flexible. Hence This section proposes and evaluate the performance of Hop Count-Based Sinkhole Attack detection Algorithm (HCOBASAA) using probability of detection, probability of false negative, and probability of false positive as the performance metrics in Software-defined wireless sensor cognitive radio network since sinkhole attack is the most common attack which can also be used to launch other attacks. On average HCOBASAA managed to yield 100%, 75%, and 70% probability of detection. the limitation of the proposed scheme is that the scheme‘s performance decreases with an increase in the attacking percentage of malicious nodes. HCOBASSA sets off the greatest probability of detection at 15% as a result of a small number of sinkhole nodes and a greater probability of false positive as the threshold is lower than most of average change in position of the legitimate nodes. In the case where malicious (sinkhole) nodes have a lower average change in position than most of the legitimate nodes, the scheme’s probability of false positive increases given a threshold which is greater than the averages. On average HCOBASSA yielded good results. However, it requires further improvements in large network sizes.

off-sensing and Route Manipulation Attack: A Cross-Layer Attack in Cognitive Radio based Wireless Mesh

In this paper, a new vulnerability in cross-layer routing protocols is discussed and demonstrated about how a perpetrator can exploit this vulnerability to manipulate traffic flow around it. Authors propose this cross-layer attack in CR-based wireless mesh networks (CR- WMNs), which is called as off-sensing and route manipulation (OS- RM) attack. In this cross-layer assault, off-sensing attack is launched at the lower layers as the point of attack but the final intention is to manipulate traffic flow around the perpetrator. Paper also introduced a learning strategy for a perpetrator, so that it can gather information from the collaboration with other network entities and capitalize this information into knowledge to accelerate its malice intentions. Simulation results show that this attack is far more detrimental than what was experienced in the past and need to be addressed before commercialization of CR-based networks. The analysis and observations not only shed light on a new kind of threats to the CR-based network, but also provided some insightful findings on how to design cross-layer protocols.

IV. ACKNOWLEDGEMENT

The author thanks Prof.S.Sridhar, Ex. Vice Chancellor, Dr.K.N.Modi University, Rajasthan, for communicating this article to this Journal for publication.

V. REFERENCES

[1]. ‘The Design of a Defense Mechanism to Mitigate the Spectrum Sensing Data Falsification attack in Cognitive Radio Ad Hoc Networks’,2016 IEEE.

[2]. A.Hyils Sharon Magdalene, Dr. L. Thulasimani,Fuzzy Clustering Means (FCM) for mitigating Spectrum sensing data falsification (SSDF) attack in Cognitive Radio Networks ‘, 2017 IEEE International Conference on Computational Intelligence and Computing Research.

[3]. Abbas Ali Sharifi and Mir JavadMuseviNiya, Member, IEEE, ‘Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach’, IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 1, JANUARY 2016 .

[4]. Alireza Attar, Helen Tang, Senior Member IEEE, Athanasios V. Vasilakos, Senior Member IEEE, F. Richard Yu, Senior

Member IEEE, and Victor C. M. Leung,Fellow IEEE, ‘A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions’, Proceedings of the IEEE | Vol. 100, No. 12, December 2012 0018-9219.

[5]. Anil Kumar and Dr. Rajendra Kumar, ‘Simulation Analysis of GLRT and Eigenvalue Based Methods for Cognitive Radio’, 2017 2ndIEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.

[6]. EI Qingqi, LI Hongning and LIU Xianjun , ‘Neighbor Detection-Based Spectrum Sensing Algorithm in Distributed Cognitive Radio Networks’, Chinese Journal of Electronics Vol.26, No.2, Mar. 2017.

[7]. Fang Ye and Xun Zhang, ‘Evidence-theory-based Collaborative Spectrum Sensing with Efficient reditability Evaluation in Cognitive Radio Networks’, 2017 Progress In Electromagnetics Research Symposium — Fall (PIERS — FALL), Singapore, 19–22 November.

[8]. GUANGMING NIE, GUORU DING (Senior Member, IEEE), LINYUAN ZHANG, AND QIHUI WU , (Senior Member, IEEE) , ‘Byzantine Defense in Collaborative Spectrum Sensing via Bayesian Learning’.

[9]. HeadarTarshBatool, Dr. R.S.Kawitkar, ‘Performance Investigation of Insistent Spectrum Sensing Data Falsification on Cognitive Radio Networks’,Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018).

[10]. Huifang Chen, Member, IEEE, Ming Zhou, Lei Xie, Member, IEEE, and Jie Li, Senior Member, IEEE, ‘Cooperative Spectrum Sensing With M-Ary Quantized Data in Cognitive Radio Networks Under SSDF Attacks’,IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 16, NO. 8, AUGUST 2017.

[11]. Huifang Chen, Member, IEEE, Ming Zhou, Lei Xie, Member, IEEE, Kuang Wang, and Jie Li, Senior Member, IEEE, ‘Joint Spectrum Sensing and Resource Allocation Scheme in Cognitive Radio Networks with Spectrum Sensing Data Falsification Attack’,IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 65, NO. 11, NOVEMBER 2016.

[12]. Ismail K. Ahmed and Abraham O. Fapojuwo, ‘Security Threat Assessment of Simultaneous Multiple Denial–of–Service Attacks in IEEE 802.22 Cognitive Radio Networks’, 2016 IEEE.

[13]. IssahNgomane, MthulisiVelempini, SabeloVelemseniDlamini, ‘ Trust-based System to Defend Against the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Network’, 2018 IEEE.

[14]. Izhar Ahmed Sohu , Asif Ahmed Rahimoon, Amjad Ali junejo, Sadam Hussain junejo,Arsalan Ahmed Sohu ‘Analogous Study of Security Threats in Cognitive Radio’, International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019.

[15]. Ji Wang,Ing-Ray Chen, Jeffrey J.P, Ding-Chau Wang, ‘SSDF Attacks in Distributed Cognitive Radio Networks’ .

[16]. Jianwu, FENG Zhiyong, ZHANG Ping,‘A Survey of Security Issues in Cognitive Radio Networks’, Beijing University of Posts and Telecommunications, Beijing 100876, China.

[17]. JIANXIN DAI , JUAN LIU, CUNHUA PAN , JIANGZHOU WANG, (Fellow, IEEE), CHONGHU CHENG, and ZHILIANG HUANG, ‘ MAC Based Energy Efficiency in Cooperative Cognitive Radio Network in the Presence of Malicious Users’, 2169-3536- 2018 IEEE,Digital Object Identifier 10.1109/ACCESS.2018.2793906.

[18]. John Kelly, Jonathan Ashdown , ‘Spectrum Sensing Falsification Detection in Dense Cognitive Radio Networks using a Greedy Method’, Air Force Research Laboratory (AFRL) Information Directorate Rome, 2019.

[19]. Jun Wu, Tiecheng Song, Cong Wang, Yue Yu, Miao Liu, Jing Hu , ‘Robust Cooperative Spectrum Sensing Against Probabilistic SSDF Attack in Cognitive Radio Networks’, National Mobile Communication Research Lab Southeast University, Nanjing, China.

[20]. Jun Wu, Xi Li, Tiecheng Song, Lei Zhang, Miao Liu, Jing Hu, ‘Two-stage Credit Threshold on Cooperative Spectrum Sensing to Exclude Malicious Users in Mobile Cognitive Radio Networks’, National Mobile Communication Research Lab Southeast University, Nanjing, China.

[21]. Lanka Sejaphala, MthulisiVelempini, SabeloVelemseniDlamini ‘HCOBASAA: Countermeasure Against Sinkhole Attacks in Software-Defined Wireless Sensor Cognitive Radio Network’, 2018 IEEE.

[22]. Linyuan Zhang, Guoru Ding, Member, IEEE, Qihui Wu, Senior Member, IEEE, Yulong Zou, Senior Member, IEEE, Zhu Han, Fellow, IEEE, and Jinlong Wang, Senior Member, IEEE, ‘Byzantine Attack and Defense in Cognitive Radio Networks: A Survey’.

[23]. Moinul Hossain and Jiang Xie, ‘Off-sensing and Route Manipulation Attack: A Cross-Layer Attack in Cognitive Radio based Wireless Mesh Networks’, IEEE INFOCOM 2018 - IEEE Conference on Computer Communications.

[24]. Natasha Saini, Nitin Pandey, Ajeet Pal Singh, ‘Analyzing and Developing Security Techniques for Worms in Cognitive Networks’, 2016 IEEE International Conference on Computational Intelligence and Computing Research.

[25]. Natasha, Nitin Pandey, Ajeet Pal Singh, ‘Formal Approach to Security Techniques in Cognitive Networks’, 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

[26]. Networks RoshniRajkumari and NingrinlaMarchang, Member, IEEE, ‘Secure Non-Consensus Based Spectrum Sensing in Non-Centralized Cognitive Radio’, IEEE SENSORS JOURNAL, VOL. 18, NO. 9, MAY 1, 2018.

[27]. Ohrid, Macedonia Pujue Wang, Cailian Chen, Shanying Zhu, Ling Lyu, Weidong Zhang, and Xinping Guan, ‘An Optimal Reputation-based Detection against SSDF Attacks in Industrial Cognitive Radio Network’, 2017 13th IEEE International Conference on Control & Automation (ICCA) July 3-6, 2017.

[28]. PinakiSankar Chatterjee,Monideepa Roy, ‘Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs’,IET Wirel. Sens. Syst., 2018, Vol. 8 Iss. 3, pp. 121-128 © The Institution of Engineering and Technology 2018.

[29]. Ping Bai, Xun Zhang, and Fang Ye, ‘Reputation-based Beta Reputation System against SSDF Attack in Cognitive Radio Networks’, 2017 Progress In Electromagnetics Research Symposium — Fall (PIERS — FALL), Singapore, 19–22 November.

[30]. Rajesh K. Sharma, Member, IEEE, and Danda B. Rawat, Senior Member, IEEE, ‘Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey’, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 2, SECOND QUARTER 2015.

[31]. Ramesh babu B, MeenakshiTripathi , Manoj Singh Gaur, Dinesh Gopalani, Dharm Singh Jat, ‘Cognitive Radio Ad-Hoc Networks: Attacks and Its Impact’.

[32]. RuiyanDu , Ying Zhou, Fulai Liu, Xinwei Wang’ ‘An Effective Collaborative Spectrum Sensing Method against SSDF Attack’, 2017 IEEE.

[33]. SasaMaric, Leonardo Goratti ‘ A Simple and Highly Effective SSDF attacks Mitigation Method’, 2016 IEEE.

[34]. ShikhamoniNath, NingrinlaMarchang and Amar Taggu, ‘Mitigating SSDF Attack using K-Medoids Clustering in Cognitive Radio Networks’, 2015 Eight International Workshop on Selected Topics in Mobile and Wireless Computing.

[35]. Shuai Yuan, Lei Li and ChunxiaoChigan, ‘On MMD-based Secure Fusion Strategy for Robust Cooperative Spectrum Sensing’, DOI 10.1109/TCCN.2019.2906236, IEEE Transactions on Cognitive Communications and Networking.

[36]. SuchismitaBhattacharjee, RaipingKeitangnao, NingrinlaMarchang, ‘Association Rule Mining for Detection of Colluding SSDF Attack in Cognitive Radio Networks’, 2016 International Conference

on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA.

[37]. Sukanya Chatterjee, Pinaki S Chatterjee A Comparison based Clustering Algorithm to Counter SSDF attack in CWSN. 2015 International Conference on Computational Intelligence & Networks.

[38]. Ting Peng, Yuebin Chen, JieXiao,Yang Zheng, Jiangfeng Yang, ‘ Improved Soft Fusion-Based Cooperative Spectrum Sensing Defense Against SSDF Attacks’, 2016 IEEE.

[39]. Xuekang Sun, Rikang Zhou, Hongxing Wu, Li Gao,Yuyan Zhang, ‘Angle based Malicious User Detection for Wideband Cognitive Radio Network’, The 20th International Symposium on Wireless Personal Multimedia Communications (WPMC-2017).

[40]. Yasir Al-Mathehaji, Said Boussakta, Martin Johnston, and HarithFakhrey,‘Defeating SSDF Attacks With Trusted Nodes Assistance in Cognitive Radio Networks’ July 19, 2017.

[41]. Yu Gan, Chunxiao Jiang, Senior Member, IEEE, Norman C. Beaulieu, Fellow, IEEE, Jian Wang, Member, IEEE, and Yong Ren, Senior Member, IEEE, ‘Secure Collaborative Spectrum Sensing: A Peer-Prediction Method’,IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 64, NO. 10, OCTOBER 2016.

[42]. Zhixu Cheng, Tiecheng Song, Jing Zhang, Jing Hu, Yazhou Hu, Lianfeng Shen, Xi Li, Jun Wu, ‘Self-Organizing Map-Based Scheme Against Probabilistic SSDF Attack in Cognitive Radio Networks’, National Mobile Communications Research Laboratory, Southeast University Nanjing, Jiangsu, 210096, China.