ISSN: 2278-4632
Vol-11 Issue-02 2021

SURVEY ON LINK LAYER ATTACKS IN COGNITIVE RADIO NETWORKS

Pappu Sharada[1], Dr. Anil Kumar Mishra
[1]*(Computer Science & Engineering, Capital Engineering College, Bhubaneswar)*
[2]*(Computer Science & Engineering, Capital Engineering College, Bhubaneswar)*

ABSTRACT

Cognitive Radio Network (CRNs) is a novel technology for improving the future bandwidth utilization. CRNs have many security threats due its opportunistic exploitation of the bandwidth. Each layer of the CRNs consisting of several attacks starting from the physical layer and moving up to the transport layer. This paper concentrates on the Link layer attacks. The future work uses Signature based Authentication Coded Intrusion Detection Scheme to detect the Byzantine attack. It works in asynchronous system like Internet and incorporates optimization to improve detection response time.

KEYWORDS

COGNITIVE RADIO NETWORK (CRN), BYZANTINE ATTACK, FUSION CENTRE, MESSAGE AUTHENTICATION CODE(MAC).

1. INTRODUCTION

Due to increasing demand of the spectrum, because of the explosive growth of wireless services, the Federal Communication Commission (FCC) has approved the unlicensed users to access the unused portion of the licensed band. This feature makes the Cognitive Radio Network. A cognitive radio network is an intelligent radio that can be programmed and configured dynamically. Its transceiver is designed to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at one location. This process is a form of dynamic spectrum management. Due to this dynamic nature there are many security threats in CRN. In this we present a solution to detect the link layer attacks such as spectrum sensing data falsification also known as Byzantine attack. As there is an IDS for the detection of attacks in physical layer, we then move on to the next layer i.e. link layer attacks. The Byzantines are the attackers and they produce a false spectrum sensing result to the secondary user and do not allow the unlicensed user to use the free spectrum band. This is also one of the Denials of service attack (DoS), so to detect this type of Byzantine attack signature based Authentication Coded Intrusion Detection Scheme is employed.

2. CATEGORIES OF THREATS IN CRN

The threats in CRN are categorized based on their layers. The physical layer attacks are of primary user emulation (PUE) attack, Objective Function attack and jamming attack. The link layer attacks comprise of spectrum sensing data falsification attack and Denial of service attack. The attacks against the network layer are sinkhole attack and HELLO flood attacks. Transport layer consisting of the Lion attack.

ISSN: 2278-4632
Vol-11 Issue-02 2021

3. DEFENDING AGAINST LINK LAYER ATTACK

Many data fusion techniques were proposed to detect the Spectrum Sensing Data Falsification (SSDF) Attack.

In [2], a Decision fusion technique is proposed in which all local spectrum-sensing results are collected and summed then it is compared to a threshold to detect an attack. Threshold value will be in between 1 and the number of sensing terminals If the sum is greater than or equal to the threshold then the result will be "Busy" i.e., it denotes the presence of the primary user. Otherwise, the result will be "free" i.e., it denotes the absence of the primary user. The major drawback in this is using of fixed thresholds. In this a problem is increasing and decreasing the threshold has major impact on the decision. Moreover, the method is ineffective in many scenarios that include multiple attackers.

In [3] Weighted Sequential Ratio Test (WSRT) is used and the Solution is composed of 2 steps: a reputation maintenance step and the actual hypothesis test. In the reputation maintenance step initially every node is assigned with the reputation value equal to zero, upon each correct spectrum report the reputation value gets increased by one. The second step is based on the Sequential Probability Ratio Test [4]. Unlike the ordinary SPRT this WSRT approach uses a trust based data fusion schemes. The drawback that exists here is there is no analytical studies have been conducted, but performance is good.

In [5] a Weight based fusion scheme is used to encounter the malicious node which transmits false sensing signals. It uses trust approach and pre-filtering techniques. Permanent malicious nodes are usually of two types such as, "Always Yes" and the "Always No". The "always Yes" type advertises the presence of the primary user and thus increasing the probability of false alarm. The other type "Always No" advertises the absence of the primary user and thus decreasing the probability of detection. This approach mainly concentrates on the pr-filtering of the data to identify the malicious user and assigning the trust factor to each user. It shows good performance result.

In [6] a Detection mechanism that runs in the fusion center. The fusion center identifies the attackers by counting mismatches between their local decision and the global decision and removes them from the data fusion process. It is robust against Byzantine attack and removes the Byzantines in a very short time span, but it works only when a centralized fusion center exists.

In [7] a Bayesian detection mechanism that requires the knowledge of priori conditional probabilities of the local spectrum sensing result and also the knowledge of priori conditional probabilities of the final sensing result. There are several combination cases exist between these two cases either correct or wrong and cost are assigned. A large cost is assigned to the wrong ones and a small cost is assigned to the correct ones. Then the overall cost is calculated by sum of all the costs weighted by the probabilities of the corresponding cases. The major drawback is that when there is an SSDF attacker the prior knowledge becomes not trustworthy, and thus the suggested detection mechanism becomes no longer optimal in terms of minimizing the overall cost.

In [8] the Neyman-Pearson Test is proposed that does not require the priori probabilities of final sensing or any cost associated with each decision case. It needs to define either maximum acceptable probability of false alarm or a maximum acceptable probability of miss detection. The other probability is minimized and the defined probability is acceptable. But, it still requires a priori conditional probabilities of the local sensing.

ISSN: 2278-4632
Vol-11 Issue-02 2021

In [9] a detection mechanism is used to detect the malicious user and it is based on the past reports. This algorithm detects the suspicious level of the secondary user based on their past reports. It calculates the trust values and the consistency values. Trust value indicator can effectively differentiate honest and the malicious secondary user. When a user turns bad then thetrust value indicator reduces the trust value. If the user behaves badly for few times then after a large number of good behaviors the trust value gets increased. If the bad behavior is consistent then it is impossible to recover. The major drawback is that the scheme cannot be applied to multiple malicious users' scenario.

4. TABLE

Table 1. Link Layer Threats, Countermeasures and Evaluations

Threats	Countermeasures	Evaluation
Spectrum Sensing Data Falsification (Byzantine attack)	Decision fusion technique where all collected local spectrum-sensing results are summed and compared to a threshold to detect an attack [2]	The major drawback is in using fixed thresholds. In this particular countermeasure increasing and decreasing the threshold has major impact on the decision. Moreover, the method is ineffective in many scenarios that include multiple attackers
	Weighted Sequential Ratio Test [3]	Solution is composed of 2 steps: a reputation maintenance step and the actual hypothesis test. No analytical studies have been conducted, but performance is good.
	Weight based fusion scheme [5]	Uses trust approach and pre-filtering techniques. Shows good performance.
	Detection mechanism that runs in the fusion center [6]	The fusion center identifies the attackers and removes them from the data fusion process. Only works when a centralized fusion center exists.
	Detection mechanism that requires a priori knowledge	The major drawback is that the a priori knowledge becomes not

ISSN: 2278-4632
Vol-11 Issue-02 2021

	[7]	trustworthy when a network is under SSDF attack, and thus the suggested detection mechanism becomes no longer optimal in terms of minimizing the overall cost
	Neyman-Pearson Test [8]	Works by defining either a maximum acceptable probability of false alarm or a maximum acceptable probability of miss detection. It still requires a priori conditional probabilities of the local sensing
	Detection mechanism based on trust	The major drawback is that the scheme cannot be applied to multiple malicious users' scenario.
Control Channel Saturation DoS Attack	Detection mechanism based on trust [9]	The suggested countermeasure adapts a trusted architecture where any suspicious CR host will be monitored and evaluated by its neighbors. A neighbor can then perform Sequential Probability Ratio Test to reach a final decision whether it is misbehaving or not. Its performance is proven to be good
Selfish Channel Negotiation	Detection mechanism based on trust [9]	Same countermeasure suggested for Control Channel Saturation DoS Attack works for this attack.

5. CONCLUSION

Signature based Authentication detects byzantine Attacks generated by malicious users and it reject false sensed data. It also reduces incorrect sensing results.CRN is less vulnerable to intrusion generated by Byzantine attacks and improves intrusion detection performance gain.

ISSN: 2278-4632
Vol-11 Issue-02 2021

FUTURE WORK

The Proposed system uses a Signature based Authentication Coded Intrusion Detection Scheme to combat Byzantine Attacks in Cognitive Radio Networks. It works in asynchronous systems like the Internet and it incorporates optimizations to improve detection response time.

Optimization replaces public-key signatures by vectors of message authentication codes during its normal operation and overcomes fundamental limitation on power of message authentication codes. Authentication has two orders of magnitude faster and providing the same level of security. Message authentication codes (MAC) uses a symmetric cryptography to authenticate communication between two parties and shares a secret session key during the communication. Sender of a message m computes a small bit string function of m and this is the key it shares withthe receiver. It then appends the string (MAC) to the message.

The receiver check the authenticity by computing the MAC in the same way and then comparing it to the one appended to the message. To compute MAC each replica and each (active) client shares a secret session key with each replica. Actually a pair of session keys for each pair of replicas. Each replica has secret session key for each client that is used for communication in bothdirections. Rather than a single session key it use a pair of keys for communication between replicas and also to allow replicas to change independently. These keys are use to verify incomingmessages.

REFERENCES

[1] Zubair Md.Fadlullah, Hiroki Nishiyama, and Nei Kato,Tohoku University Mostafa M.Foda, (2013), "Intrusion Detection System (IDS) for combating attacks in cognitive radio networks", IEEE network,vol. 27, pp.51-56.
[2] A. Pandharipande et al., (2005), IEEE P802.22 "Wireless RANs: Technology Proposal Package for IEEE 802.22", IEEE 802.22 WG on WRANs.
[3] Ruiliang Chen, Jung-Min Park, Y. Thomas Hou and Jeffrey H. Reed, (2008), "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks", IEEE Communications Magazine, Vol.46, pp.50-55.
[4] Yeelin Shei and Y. T. Su, (2008), "A Sequential Test Based Cooperative Spectrum Sensing Scheme for Cognitive Radios", IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008), pp.1-5.
[5] Praveen Kaligineedi, Majid Khabbazian and Vijay Bhargava. K , (2008), "Secure CooperativeSensing Techniques for Cognitive Radio Systems", IEEE International Conference on Communications (ICC), Beijing, China, pp.3406-3410.
[6] Ankit Rawat, Priyank Anand, Hao Chen and Pramod Varshney, (2010), "Countering Byzantine Attacks in Cognitive Radio Networks", 2010 IEEE International Conference on Acoustics Speech andSignal Processing (ICASSP), Dallas, TX, pp.3098-3101.
[7] Linjun Lu, Soo-Young Chang et al., (2006), "Technology Proposal Clarifications for IEEE 802.22 WRAN Systems", IEEE 802.22 WG on WRANs.
[8] Joerg Hillenbrand, Timo Weiss and Friedrich K. Jondral, "Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems", IEEE Communication Letters, Vol.9, No.4, 2005, pp.349-351.
[9] Wenkai Wang, Husheng Li, Yan Sun and Zhu Han, (2009), "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks", 43rd Annual Conference on Information Sciences and Systems, 2009 (CISS 2009), Baltimore, pp.130-134.