IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Security Based Hostile User Detection in Cognitive Radio Networks

Reshma Rajan[1], Syamesh K G[2], Anjali Raj[3], Jeethumol K Joy[4]

M.Tech Student, ECE, College Of Engineering Kidangoor, Kottayam, India [1, 3, 4]

Assistant Professor, ECE, College Of Engineering Kidangoor, Kottayam, India[2]

Abstract: The extensive threats in cognitive radio networks is detection of primary user signal. Cooperation among secondary users swell the performance of the system significantly. In cooperative sensing in hostile environments, intruder nodes send incorrect sensing results to the SBS and make the fusion center erroneously decides about the presence of the primary user. Here we proposed a novel active transmissions based algorithm with ECC for detecting such malicious SUs. This is the first algorithm that can proactively detect malicious SUs, thereby preventing Cognitive Radio Networks from making incorrect sensing decisions. This helps in reducing the interference to Primary Users as well as increases the accuracy of sensing. Elliptic Curve Cryptography (ECC) is used for the security in the CR network. ECC key sizes are shorter than that of RSA keys, the length of the public key and private key is much shorter in elliptic curve cryptosystems. ECC reduces the throughput loss and provides security to the networks.

Keywords: Cognitive radio, cooperative spectrum sensing, Primary User Emulation (PUE), Elliptic curve cryptography (ECC).

I. INTRODUCTION

The ample growth of wireless communications leads to the insufficiency of frequency spectra and available radio spectrum is a limited natural resource, being unified day by day. Cognitive radio is a technique where secondary user looks for a free band to sense when primary user does not use its licensed band. it is possible through spectrum sensing[1] and three types of spectrum sensing are co-operative sensing[2], interference based sensing, and non cooperative sensing. The frequency bands which are not occupied by PUs is called white space or spectrum holes. Cognitive network is sensitive to preservation threats. The attackers may be external users or secondary users act as a malicious users. So, in order to overcome these problems, hostile user detection system is used. Cooperative sensing improves sensing accuracy but makes the system more sensitive to hostile users that may be instant in the system. In cooperative spectrum sensing (CSS), multiple secondary users (SUs) conspire to effectively expose a primary user (PU). However, the cooperation among SUs increases concerns about reliability and security of cooperative spectrum sensing, as any of the SUs may report incorrect sensing data. The apocryphal reported data can easily issue the spectrum sensing decision taken by the fusion centre. The pollution of data may establish either by malfunctioning of SUs or by intentional administration of data by assured SUs, called hostile users. The data reported by malfunctioning SUs may differ from the actual data.

A hostile user may (i) have a hardware defect due to which its readings are erratic; (ii) be hacked by the owner so that it addresses erratic sensing results without performing any sensing to save time and energy; (iii) report the channel to be busy so as to either consent the channel free for its own usage [3] or to initiate a Denial- of-Service attack across the network [4]; (iv) miserly report the channel to be free so that it can sense on that channel; or, (v) skip in-band sensing as save energy and throughput. The recent increase in attacks against TCP Protocol[5], mobile devices or other metalware devices [6] and the software based design of CRs suggests that in the future CRs will be very sensitive to hostile user's attacks. Such attacks may affect the sensing capability of CRs and may result in nodes lead to interference to Pus. One of the most common techniques for detecting hostile users is based on the supposal that neighboring CRs have identical readings. These techniques uses a passive approach that detects hostile users when sensing the channel for the presence of PUs. This technique converge readings from all CRs and then signs those nodes as hostile whose readings differ from their neighbors.

II. COGNITIVE RADIO NETWORKS

An infrastructured network of CRs (Fig I) where multiple nodes (or Secondary Users, SUs) may be associated with a secondary Base Station (SBS) and the position of SUs is unknown. Though cognitive radio was initially thinking of as a software-defined radio most research targets on spectrum-sensing cognitive radio. The chief problem in spectrum-sensing cognitive radio is designing immense quality spectrum-sensing devices and algorithms for rearranging spectrum-sensing data between nodes. It has been shown that a hasty energy detector cannot guarantee the exact detection of signal presence,[9] calling for more precise spectrum sensing techniques and requiring data about spectrum sensing to be regularly exchanged between nodes. Incrementing the number of cooperating sensing users decays the possibility of false detection. CR can

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

sense its environment , can adapt to the user's communications needs while harmonious to FCC rules in the United States. In theory, the number of spectrum is infinite; practically, for propagation and other reasons it is limited because of the grace of certain spectrum portions. Assigned spectrum is far from being fully used, and efficient spectrum use is a viable concern; CR offers a solution to this problem. A CR can intelligently detect whether some part of the spectrum is in use, and can transiently use it without interfering with the transmissions of other users.

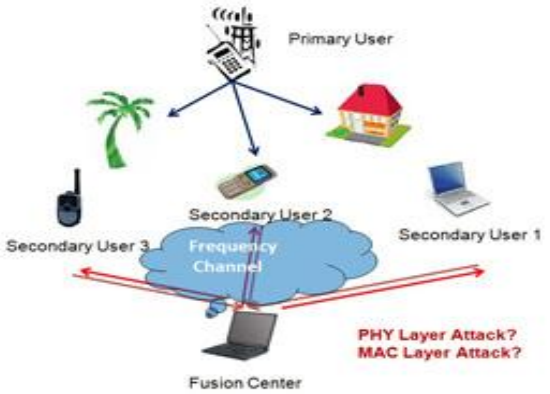

Figure I. Cognitive Radio Networks

III. ALGORITHM: OVERVIEW

Algorithm [12]can be used to find the hostile user present in the cognitive radio networks. Cognitive radio conducts various sensing tests by sensing server and neighbor node is tested by transmitting primary user emulation (PUE) signals. Based on the received signal strength report obtained from the node which is tested, it is possible to estimate whether this node is hostile or not. The tests can be strongly delivered to nodes before the actual sensing needs to be done, Algorithm [12] used proactive approach to detect hostile users.

The detection process is more accurate because of the following reasons:

• Secondary user base station(SBS) have entire knowledge about the ground truth (e.g. transmission power level and path loss information) for the tests, thus it can more exactly conclude if the received power level reported by a receiver is correct or not.
• Information of received signal strength at a receiver for a given transmitter are compared with the earlier readings for the same transmitter receiver pair. This is very useful for detect the malicious users in the cognitive.

For finding the hostile users, first selects a channel c_i which is free over the testing is to be performed. All nodes in the network have a reputation values[12] ρ_i which is equal to the expected probability of a node being malicious. Algorithm then proceeds in multiple time slots and in each time slot a subset of nodes is tested. After that SBS computes testing schedule S, which is a set of tuples (n_i, n_j, T_j, t_l) representing that n_j tests n_i in slot t_l by transmitting at a power level T_j.SBS then computes the probability of each node Pi and check whether pi is less than threshold reputation value β which is the average of reputations values of the nodes in the subset. If $P_i \leqslant \beta$ then the node is malicious otherwise the node is non-malicious. Sometimes we cannot determine whether the readings is correct or not, then we cannot ensure that the detection is correct or not. For avoiding this problem SBS computes the expected pathloss between a pair of nodes varies approximately linearly with the log of frequency [9], therefore using the following equation, and the values of a_{ij} and b_{ij}, it is possible to arrive at expected path loss (P^e_{ij}) from n_i to n_j for any frequency f:

$$P^e_{ij} \approx a_{ij} \log f + b_{ij}$$

The value of aij and bij have been shown to depend on the environment, therefore algorithm computes it as it proceeds. The values of observed path loss (Pij) may be different from the expected path loss (Pe ij) due to either the noise associated with this transmission or because nj is maliciously reporting incorrect readings, then the node is considered as malicious. If the observed pathloss is similar to expected pathloss, then the node is not a malicious one. After that process, check the expected and received power level reported by node nj and if the power level is less than or equal to noise floor level, then the node is not a hostile user and renew the reputation value of all secondary users. Otherwise it persuade node is malicious.

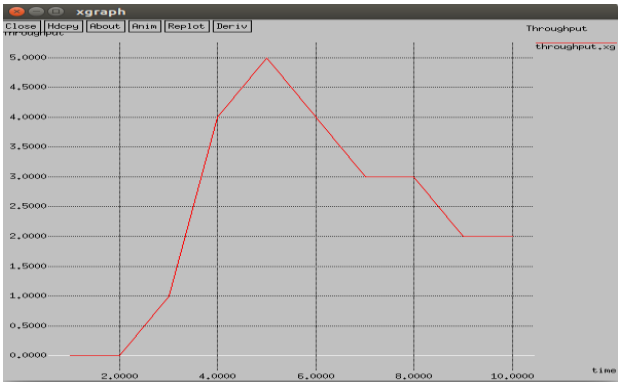

Figure II: Variation of throughput in cognitive radio networks with hostile users

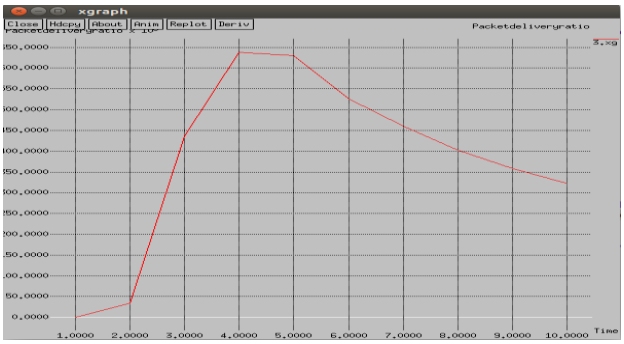

Figure III : Variation of packet delivery ratio in cognitive radio networks with hostile users

From figure (II &III)the value of throughput and packet deliver ratio are decreases when the hostile users are present in the networks. That means due to the presence of hostile users the data packets cannot reaches the correct

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

destination that affects the packet loss in the network. So these algorithm does not provides security to the network. For providing security and maintaining the values of throughput we suggests a method, which uses cryptographic techniques with proposed algorithm.

IV. SECURITY SOLUTION TO DEFEND MALICIOUS BEHAVIOR

Security can be provided by the methods of Cryptography, Protocols, Intrusion Detection System (IDS) and Trusted Third Party (TTP)[17]. In cognitive radio Network, the data is sent using cryptography [13] and the security can be provided through this method.Cryptography means to conversion of (or encrypt) the electronic data (which is to be send) into another pattern called ciphertext, which cannot be easily understood by anyone expect authorized users. Even if the malicious user accesses the data, it should not be able to understand the content of it. Cryptography can be symmetric (which uses same key for both encryption and decryption of the message) and asymmetric (which uses one key to encrypt and other to decrypt the message).This security preserves the integrity and confidentiality of data. Techniques like Elliptic curve cryptography (ECC) and RSA are used to preserve the security principles. To face cryptographic attacks, one of most efficient methods is the Elliptic curve cryptography (ECC). ECC [16] is an approach to doing asymmetric cryptography. The censuring feature of asymmetric cryptography is this key pair which provides the fact that one of the keys cannot be obtained from the other. By giving each node public and private keys, we can ensure that the communication between the nodes will be very secret, and no one can view the message, or the forwarding nodes neither the attacker nodes.

ECC is said to be one of the most efficient methods of cryptography. It is Asymmetric cryptography, which is a powerful and essential technology. The ability to distribute public keys and communicate securely over an open network is truly revolutionary. ECC bids greater security for a given key size. The smaller key size also makes possible much more solid implementations for a inured level of security, which means faster cryptographic operations, running on smaller chips or more solid software. This means limited heat production and limited power consumption.

Its inverse operation gets harder, faster, against increasing length of key than do the inverse operations in Diffie Hellman [16] and RSA. This keeps ECC implementations smaller and more efficient. ECC can use shorter key and offer the same level of security as other asymmetric algorithms using much better ones.

Moreover, the gulf between ECC and its competitors in terms of key size needed for a given level of security becomes fiercely more pronounced, at higher levels of security [19]. Table 1 shows the differences between the public key sizes[20]; we can conclude that ECC key is the shortest one.

TABLE I NIST RECOMMENDED KEY SIZES

Symmetric Key Size (bits)	*RSA and Diffie-Hellman Key Size (bits)*	*Elliptic Curve Key Size (bits)*
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

The mathematical operations of ECC[17] is describe over the elliptic curve $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$. All value of the 'a' and 'b' gives a different elliptic curve. Each points (x, y) which amuses the above equation surplus a point at infinity lies on the elliptic curve. Key generation is an important part where we have to generate both public key and private key[17]. Every user has a public and a private key. Public key is used for encryption/signature verification. Private key is used to decryption/signature generation. The central part of any cryptosystem involving elliptic curves is the elliptic group. All public-key cryptosystems [18] have some underlying mathematical operation.ECC has point multiplication (repeated addition of two points).Both source and destinations agree to some publicly-known data items like the elliptic curve equation ,values of a and b and prime, p . The elliptic group computed from the elliptic curve equation, base point B, taken from the elliptic group similar to the generator used in present cryptosystems. Each user generates their asymmetric keys.

Private Key ,x = an integer, selected from the interval [1, p-1]

Public Key ,Q = product of private key and base point

$$Q = x*B$$

Suppose Source n_i wants to send to destination n_j an encrypted message .Both source and destination node agree on a base point, B, and creates their public/private keys .Suppose n_i's Private Key = a and their Public Key = $P_A = a * B$ .And n_j's Private Key = b and their Public Key = $P_B = b * B$

Source node ni takes plaintext message, M, and encodes with its public key onto a point, P_M, from the elliptic group,ni chooses other random integer, k from the interval [1, p-1]. The ciphertext is a pair of points

$$P_C = [(kB), (P_M + kP_B)]$$

To decrypt, destination node computes the product of the first point from PC and this private key, b ie,b * (kB) and then takes this product and subtracts it from the second point from PC

$$(P_M + kP_B) – [b(kB)] = P_M + k(bB) – b(kB) = P_M$$

Destination node n_j then decodes PM to get the message, M.

Since the ECC key sizes[20] are shorter than that of RSA keys, the length of the public and private key is much shorter in elliptic curve cryptosystems. This results faster

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

processing times, and lesser demands on memory and bandwidth.Some studies have found that ECC is faster than RSA for encryption and decryption.ECC is particularly useful in applications where memory, bandwidth, and computational power is limited.

V. SIMULATION RESULTS

The simulation of algorithm is carried out by using NS2, we evaluated the performance of proposed algorithm and compared it with state of the art solutions. In the simulation, we deployed varying number of SUs in a field of size 1670x970 as SBS may have a range of as much as 100km [4]. Table II gives the default values of various parameters used during the simulation. Each simulation was performed 100 times and the average along with 95 percentage confidence interval is plotted. In order to avoid testing SUs when not required, the SBS initiated testing schedule through algorithm only after size of the set A was at least 20 percentage of the total number of SUs associated with SBS. The mobility pattern of the SUs was simulated using data from [17]. Obstacles were deployed in the network and the slow fading due to obstacles was modeled [2]. To account for the fast fading due to thermal noise, a Gaussian noise with zero mean and variance of 1 dB [1] was also introduced on all paths.

TABLE III SIMULATION PARAMETERS

Parameter	Value
Field Size	1670x970
Number of SUs	45
Number of PUs	2
Number of malicious SUs	5
β	1

The algorithms based on this technique collect readings from all CRs and then spot those nodes as hostile whose readings differ significantly from their neighbors. Elliptic curve cryptography (ECC)[17] is used for the security in CR networks.

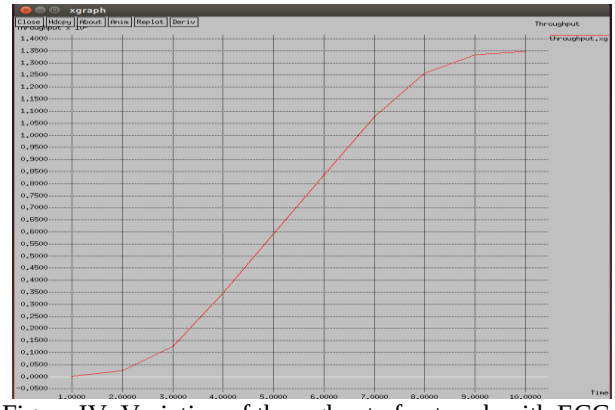

Figure IV: Variation of throughput of network with ECC.

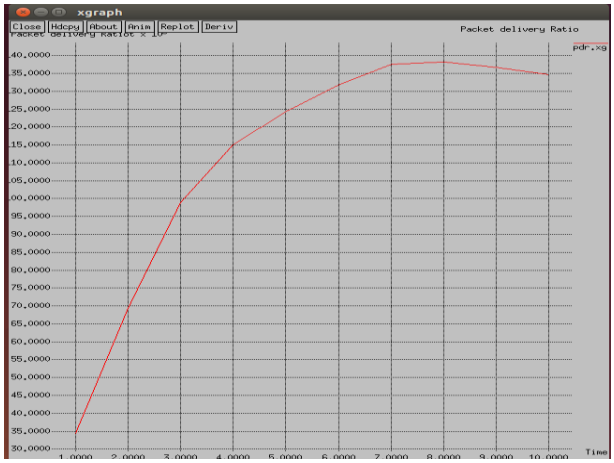

Figure V: Variation of Packet Delivery Ratio of network with ECC.

Throughput loss per user, which define as the average fraction of time spend by SUs receiving data related to sensing. The simulation shows that throughput is increased when using the elliptic curve cryptography. In the case of packet delivery ratio, simulation result shows that is reduced when ECC is added to the CR network. Fig. IV &V shows the plot of variation of throughput and packet delivery ratio with ECC.

VI. CONCLUSION

Cognitive network is precise to security hazards. The attackers may be external users or secondary users acting as a malicious user. So, in order to overcome these issues malicious user detection system is used. Compared with existing algorithms which are reactively detect hostile SUs proposed algorithm [12] , a novel active transmissions based algorithm for detecting such malicious SUs. This is the first algorithm that can proactively detect malicious SUs, thereby preventing Cognitive Radio Networks from making incorrect sensing decisions. This helps in reducing the interference to Primary Users as well as increases the accuracy of sensing. This algorithm [12]reduces the throughput loss due to sensing by as much as 65% while achieving higher accuracy compared to existing algorithms. The simulation results shows that proposed algorithm with ECC reduces the throughput loss and provides security to the networks.

REFERENCES

[1] H. Kim and K. G. Shin, "In-band Spectrum Sensing in Cognitive Radio Networks: Energy Detection or Feature Detection",in Proc. of ACM MobiCom, 2008.

[2] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing Among Cognitive Radios", in Proc. of IEEE ICC, 2006.

[3] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System", IEEE TWC, vol. 9, no. 8, pp. 2488–2497, 2010.

[4] O. Fatemieh, A. Farhadi, R. Chandra, and C. Gunter, "Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks", in Proc. of NDSS, 2011

[5] A. W. Min, K.-H. Kim, and K. G. Shin, "Robust Cooperative Sensing via State Estimation in Cognitive Radio Networks", in Proc. of IEEE DySPAN, 2011.

[6] T. Bansal, B. Chen, and P. Sinha, "DISCERN: Cooperative Whitespace Scanning in Practical Environments", in Proc. of IEEE INFOCOM, 2013

[7] A. Min, K. Shin, and X. Hu, "Attack-Tolerant Distributed Sensing for Dynamic Spectrum Access Networks",in Proc. of IEEE ICNP, 2009 [8] W. Min, K. G. Shin, and X. Hu, "Secure Cooperative Sensing in IEEE 802.22 WRANs Using Shadow Fading Correlation", IEEE Transactions on Mobile Computing, 2010.

[9] O. Fatemieh, R. Chandra, and C. Gunter, "Secure Collaborative Sensing for Crowd Sourcing Spectrum Data in White Space Networks",in Proc. of IEEE DySPAN, 2010.

[10] H Li and Z. Han, "Catch Me If You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks", IEEE Transactions on Wireless Communications, vol. 9, no. 11, pp. 3554–3565, 2010.

[11] W. Wang, H. Li, Y. Sun, and Z. Han, "Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks", EURASIP Journal on Advances in Signal Processing, 2010

[12] T. Bansal, B. Chen, and P. Sinha, "Malicious User Detection in Cognitive Radio Networks Through Active Transmissions", Tech. Rep., http://www.cse.ohio-state.edu/∼bansal/FastProbeTechRep.pdf.

[13] Kiyomichi Araki, Takakazu Satoh and Shinji Miura. "Overview of Elliptic Curve Cryptography", Lecture Notes in Computer Science Vol.1431, 1998.

[14] C.S. Hyder, B. Grebur, and L. Xiao,"Defense against spectrum sensing data falsification attacks in cognitive radio networks," in Security and Privacy in Communication Networks. Springer, 2012, pp. 154-171 [15] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in Proc. IEEE International Conference on Communications (ICC), 2009, pp. 15.

[16] E. AL-DAOUD, R. MAHMOD, M. RUSHDAN, AND A. KILICMAN. A new addition formula for elliptic curves over GF(2n). IEEE Transactions on Computers, 51:972–975, 2002.

[17] Darrel Hankerson. Guide to Elliptic Curve Cryptography. Springer, 2004.

[18] Neal Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203 – 209, 1987.

[19] Martin Leslie. Elliptic curve cryptography. (An ECC research project), 2006.

[20] M. Brown, D. Hankerson, J. Lopez, A. Menezes, Software Implementation of the NIST Elliptic Curves Over Prime Fields, 2001, http://citeseer.ist.psu.edu/brown01software.html