International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 1 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195164

Accessing Network Using Secure Android Applications

R. Gomathyjayam[1], R. Thilakavathi[2]

[1]Professor, Department of Computer Applications, Bon Secours College for Women, Thanjavur, Tamil Nadu, India

[2]M.Sc., Department of Computer Science, Bon Secours College for Women, Thanjavur, Tamil Nadu, India

ABSTRACT

Security plays a vital role in today's mobile world. There are security issues like sniffing of data while accessing information through open channel. Proper security measures can help to deal with the common security threats faced by mobile phone users such as data protection, privacy, application and personal information security. Cryptographic techniques play an important role in protecting communication links and data, since access to data can be limited to those who hold the proper key. This paper discusses a method to securely access information in a network by an android mobile application using AES cryptographic technique. The paper describes a new key sharing algorithm, based on the symmetric key management, for faster and efficient encryption of data that is suitable for use in a mobile device.

Keywords : Cognitive Radio Networks, Primary User, Secondary Users.

I. INTRODUCTION

The telecommunications network allows computers to exchange data. The connections between nodes are established using either cable media or wireless media. Network computer devices that originate, Route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission media used to carry their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent. In most cases, communications protocols are layered on (i.e. work using) other more specific or more general communications protocols, except for the physical layer that directly deals with the transmission media network support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications

II. LITERATURE SURVEY

Reputation and Trust Management

The reputation based frameworks are the nodes maintain reputations of other nodes and evaluate their trustworthiness are deployed to provide Scalable, Diverse and for countering different types of misbehavior resulting from malicious selfish nodes in the networks. The author (Jaydip et al.,2009) is proposed that Reputation systems are described along with their unique characteristics and working principles. Reputation and trust are very useful tools that are used to facilitate decision making Reputation is the opinion of one entity about another it signifies

the trustworthiness of an entity. Trust is the expectation of one entity about the action of another. Reputation and trust have been adapted to wireless communication Network it can solve many problems in the Networks.

Combinationarial Optimization dentification Algorithm (Coi)

The COI (Combinationarial Optimization Identification Algorithm) to defend against such attacks .Cooperative Spectrum sensing has been shown good performance in improving the accuracy of primary user detection .zhenquiri et al., 2013 proposed a modified Design an attack model,called cooperative attack in which an attacker injects self-consistent false data to multiple sensors simultaneously. A theorem that the center node of a cognitive radio network may face uncertainties under a cooperative attack, especially in the case when a large portion of sensors are compromised. A modified COI algorithm to deal with cooperative attacks. Our algorithm is a good scheme to complement IRIS for cooperative attacks, and can be flexibly adjusted to fulfill the detection delay requirement. Intensively evaluate our algorithm through simulation, with the results validating its performance. The original COI is an approach for identifying multiple instances of bad data in power system state estimation. The essential idea is to construct a partial decision tree using the branch-and-bound method to obtain a feasible solution with the minimum number of bad data.

Clustered Based Algorithms

The spectrum sensing methods can be distributed in three categories i.e. transmitter, receiver. (Dr. Talat Altaf et al.,2013) is propose cluster based algorithms is based spectrum sensing and interference-temperature based detection algorithms. From these, transmitter detection based methods are a preferred way of sensing for presence/absence of spectral holes. These methods can be implemented through various techniques including coherent detection, feature detection and energy based detection algorithms. Coherent sensor is an optimal linear detector for known primary signals in presence of white Gaussian noise. However, detector implementation requires. Demodulation of received signals for achieving the optimal gains.

Agent-Based Trust Calculation

The author (yenumula B.Reddy et al., 2011) is proposed agent based approach algorithm. The Cooperation in wireless sensor networks to detect the malicious node without any Infrastructure is a recent trend in research. The current models need more storage, Computation, security tools and communication requirements. The fail wireless sensor Network due to limitation of resources. The proposed agent based approach eliminates the computations in the sensor nodes with appropriate trust factor. The proposed approach uses an agent based collaborative concept ensure the trust in the successive node in the Path. The proposed agent based framework uses reputation of neighboring node as part of trust calculation in its successive node.

Sophisticated Detection Methods

The Spectrum scarcity is becoming a major issue for service providers interested in either deploying new services or enhancing the capacity for existing applications. The author (Amir Ghasemi et al.,2007)is proposed that Recent Measurements suggest that many portions of the licensed (primary) spectrum remain unused for significant periods of time. Sensing-based access incurs a very low infrastructure cost and is backward compatible with the legacy primary systems.

III. EXISTING PROCESS

The T-CSS (Traditional collaborative spectrum sensing) protocol delays in data transmission and unaware of secondary user selection for licensed bandwidth and interference occur in unlicensed

secondary network, it lack in secondary power, not able to detect weak primary signals, in order to protect primary receivers from interference. By proposing an energy efficient CSS protocol, namely energy efficient collaborative spectrum sensing EE-CSS protocol is used to transmit the data efficiently. EE-CSS attempts to reduce the number of transmitted reports from HSUs, based on the observation that HSUs agree on the spectrum usage more often than they disagree. CRN is to utilize the unused licensed spectrum opportunistically. The SUs should protect the accessing right of the PUs whenever necessary.

IV. PROPOSED METHODOLOGY

The architecture consists of the following system entities.

I.primary user: A user who has higher priority or legacy rights on the usage of a specific part of the spectrum. Primary user provides path or channel to the secondary users

ii.secondary user: secondary user base station(SUBS)transmit the data and reception is done by honest secondary users(HSUs)secondary user

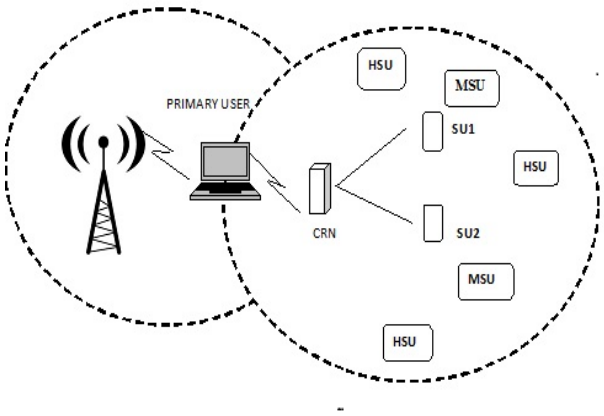

Figure 1. Proposed System Architecture

iii. Honest secondary user:

The person who is receiving the data from the secondary user base station is said to be honest secondary user.

V. IMPLEMENTATION RESULTS

COGNITIVE RADIO NETWORK

Cognitive techniques have been used in wireless networks to circumvent the limitations imposed by conventional WSNs. Cognitive radio (CR) is a candidate for the next generation of wireless communications system. The cognitive technique is the process of knowing through perception, planning, reasoning, acting, and continuously updating and upgrading with a history of learning. If cognitive radio can be integrated with wireless sensors. CR has the ability to know the unutilized spectrum in a license and unlicensed spectrum band, and utilize the unused spectrum opportunistically. The incumbents or primary users (PU) have the right to use the spectrum anytime, whereas secondary users (SU) can utilize the spectrum only when the PU is not using it.

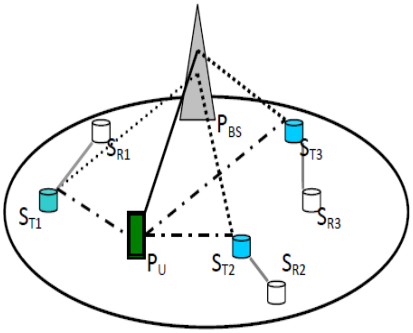

Figure 2. Cognitive radio Network

COLLABORATIVE SPECTRUM SENSING TECHNIQUE

In this spectrum is used to detect spectrum band for transformation and reception. The matched filter detection technique requires a demodulation of the PU's information signal, such as the modulation type and order, pulse shaping, packet format, operating frequency, bandwidth, etc. CR Network sensing receive information from the PU's pilots, preambles, synchronization words or spreading codes etc in figure 4.4. The advantage of the matched filter method is that it takes a short time and requires fewer samples of the received signal. Sensing reports

provided by SUs for a given licensed band may differ due to differences in channel fading gains, locations of SUs and primary network transmitters, number of signal energy quantization levels used at the sensing SU, and sensing errors.

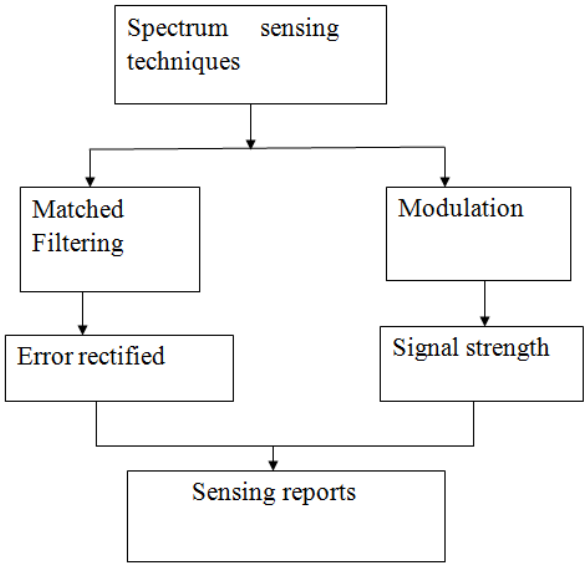

Figure 3. Collaborative spectrum sensing technique

COOPERATIVE TRUST MANAGEMENT AND AVOID MALICIOUS BEHAVIOR

CR Network sensors may encounter incorrect judgments because radio-wave propagation through the wireless channels has adverse factors, such as multi-path fading, shadowing, and building penetration. In addition, CR wireless sensors are hardware constraints and cannot sense multiple channels simultaneously. It has a malicious behavior to intermediate the signal spectrum. TRMSs record the accuracy of previous sensing reports sent by SUs and compute a trust value for each SU which is taken as the trustworthiness of its future sensing reports. And encounter the reports from SUs may be required to mitigate against the effects of malicious behavior of MSUs in figure 4.5. Therefore, CR wireless sensors cooperate and share their sensing information with each other to improve the sensing performance and accuracy.

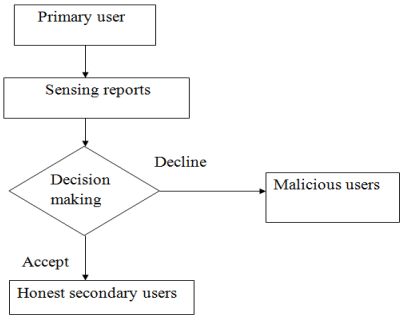

Figure 4. Cooperative Trust Management and avoid malicious behavior

PRIORITY BASED SPECTRUM TRANSFORMATION

In Cognitive Radio network the users are classified into Licensed Primary Users and Unlicensed Secondary Users and there is no dedicated channel to send data, sensors need to negotiate with the neighbors and select a channel for data communication in CR-WSNs in figure 4.6. This is a very challenging issue, because there is no cooperation between the PUs and SUs. PUs may arrive on the channel any ime. If the PU claims the channel, the SUs have to leave the channel immediately. CRN is implemented for short range wireless applications such as wireless sensor networks (WSNs) such wireless and Bluetooth, where the transmission distance is usually small (e.g., tens of meters the steady-state average total number of sensing reports transmitted for each band And assume that the packets transmitted from the FC and SUs are of equal length in both EE-CSS and T-CSS.

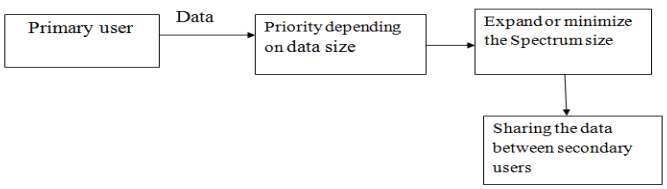

Figure 5. Priority based spectrum Transformation

VI. CONCLUSION

Cognitive Radio (CR) is an adaptive, intelligent radio and network technology that can automatically detect available channels in a wireless spectrum and change transmission parameters enabling more communications to run concurrently and also improve radio operating behavior. Cognitive radio uses a number of technologies including Adaptive Radio (where the communications system monitors and modifies its own performance) and Software Defined Radio (SDR) where traditional hardware components including mixers, modulators and amplifies have been replaced with intelligent software. A spectrum sensing scheme, was proposed to improve the utilization efficiency of the radio spectrum by increasing detection reliability and decreasing sensing time. The proposed scheme presented spectrum sensing in effective manner So the priority based and security-based spectrum sensing is produced. This system also implemented in hardware successfully.

VII. FUTURE ENHANCEMENT

Wireless technology is proliferating rapidly, and the vision of pervasive wireless computing and communications offers the promise of many societal and individual benefits. While consumer devices such as cell phones, PDAs and laptops receive a lot of attention, the impact of wireless technology is much broader, e.g., through sensor networks for safety applications and home automation, smart grid control, medical wearable and embedded wireless devices, and entertainment systems. This explosion of wireless applications creates an ever-increasing demand for more radio spectrum. However, most easily usable spectrum bands have been allocated, although many studies have shown that these bands are significantly underutilized. These considerations have motivated the search for breakthrough radio technologies that can scale to meet future demands both in terms of spectrum efficiency and application performance.

VIII. REFERENCES

[1]. A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in Proc. IEEE DySPAN, 2005, pp. 131-136.

[2]. A. Ghasemi and E. Sousa, "Opportunistic spectrum access in fading channelsthrough collaborative sensing," J. Commun., vol. 2, no. 2, pp. 71-82, Mar. 2007.

[3]. S.Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201-220, Feb. 2005.

[4]. J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," IEEE Pers. Commun., vol. 6, no. 4, pp. 13-18, Aug. 1999.

[5]. E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: A point system," in Proc. IEEE VTC Spring, 2010, pp. 1-5.

[6]. G. Staple and K. Werbach, "The end of spectrum scarcity," IEEE Spectr., vol. 41, no. 3, pp. 48-52, Mar. 2004.

[7]. H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc. IEEE, vol. 98, no. 10, pp. 1755-1772, Oct. 2010.

[8]. T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," IEEE Commun. Surveys Tuts., vol. 11, no. 1, pp. 116-130, 2009.

[9]. W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: Detect malicious nodes in collaborative spectrum sensing," in Proc. IEEE GLOBECOM, 2009, pp. 1-6.

Cite this article as : R. Gomathyjayam, R. Thilakavathi, "Accessing Network Using Secure Android Applications", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 1, pp. 438-442, January-February 2019. Available at doi : https://doi.org/10.32628/CSEIT195164
Journal URL : http://ijsrcseit.com/CSEIT195164