Simulation Framework for Security Threats in Cognitive Radio Networks

Elena Romero, Alexandre Mouradian, Javier Blesa, José M. Moya, Alvaro Araujo
Universidad Politécnica de Madrid, ETSI Telecomunicación,28040 Madrid, Spain
{elena,alex,jblesa,josem,araujo}@die.upm.es

Abstract

Along with Cognitive Radio Networks are been developed, to design optimistic security mechanisms is becoming a big challenge. This paper proposes a taxonomy of attacks on Cognitive Radio Networks. This will help researches in the area to better understand the security problems and design more optimistic countermeasures. A new simulation framework for security threats has been developed to check all these attacks and countermeasures. Simulation framework has been tested with a Primary User Emulation attack. A new testbed for simulations suitable for CR security is ready.

1 Motivation

The wireless communications evolution followed in recent years has an intrinsic problem: the growing scarcity of spectrum. With the Cognitive Radio (CR) definition, it is attempted to solve this problem by using the spectrum dynamically.

CR allows efficient use of available spectrum by defining of two types of users in wireless networks: licensed and unlicensed users. An unlicensed user (also called Secondary User (SU)) can use the spectrum if it is not being used at that time by licensed users (also called Primary User (PU)). When the licensed user appears to use the spectrum, unlicensed user must find another spectrum to use [1].

Despite cognitive radio is an active field of research, security aspects have not yet been fully explored even though security will likely play a key role in the long-term commercial viability of

the technology. The security paradigms are often inherited from classic networking and do not fit with the specifications of cognitive radio networks. Although there is not lot of literature about this topic, lately, researchers has seen that cognitive radio has special characteristics that makes its own security an interesting research field, since more chances are given to attackers by cognitive radio technology compared to general wireless network. However, at present there are no specific secure protocols for cognitive radio networks.

At this point in the still immature point of cognitive radio networks, it is important understand some key fundamental issues as the potential threats, the potential attacks and the consequences of these attacks.

The CR nature of the system introduces an entire new suite of threats and tactics that are not easily mitigated. The two main characteristics of cognitive radio are environment awareness and learning and acting capacity. In principle, these characteristics should be an advantage against attacks but they can become in weaknesses. For example, cognitive radio nodes collaborate to make better decisions but the communications are a means to propagate the attack in the network.

Looking these two characteristics since the attacker point of view, the fundamental differences between a traditional wireless network and the CR network are:

- The potential far reach and long-lasting nature of an attack.
- The ability to have a profound effect on network performance and behavior through simple spectral manipulation.

The information sensed in a CRN is used to construct a perceived environment that will impact in a certain way the current and future behaviors of all the nodes in the network. The induction of an incorrectly perceived environment will cause the CRN to adapt incorrectly, which affects short-term behavior but also because of their ability to learn, propagate the error to the new behaviors. Thus, the malicious attacker has the opportunity for long-term impact on behavior. Furthermore, the CR

collaborates with its fellow radios to determine behavior. Consequently, this provides an opportunity to propagate a behavior through the network.

Looking through the features of CRN one by one as done in [2], it can be detected threats associated with each one of them:

- **Maintains awareness of surrounding environment and internal state**. It could be an opportunity for spoofing that will send malicious data to the environment to provoke an erroneously perception
- **Adapts to its environment to meet requirements and goals**. It is an opportunity to force desired changes in behavior in the victim.
- **Reasons on observations to adjust adaptation goals**. It could be an opportunity to influence fundamental behavior of CRN
- **Learns from previous experiences to recognize conditions and enable faster reaction times**. Opportunity to affect long-lasting impact on CR behavior
- **Anticipates events in support of future decisions**. It could be an opportunity for long-lasting impact due to an erroneous prediction
- **Collaborates with other devices to make decisions based on collective observations and knowledge**. It is an opportunity to propagate an attack through network.
- **Wireless communication**. Data might be eavesdropped and altered without notice; and the channel might be jammed and overused by adversary. Access control, confidentiality, authentication and integrity must be guaranteed.

In the other hand, CRN features serve too to mitigate malicious manipulation. CRN have:

- The ability to **collaborate** to authenticate the local observations that are used to form perceived environments
- The ability to **learn** from previous attacks.
- The ability to **anticipate** behaviors to prevent attacks.

- The ability to perform **self analysis of behavior**

In this context it is easy to understand that ensuring the security of CRN is crucial to its future as a technology to deploy. Therefore, it is important to test the security of such kind of networks against the potential threats. In this way, although some work has been developed, there is not a platform to check whether a network is resilient against different attacks. A complete test-bed to simulate attacks and countermeasures is essential for the future of this technology.

The organization of this paper is as follows: In Section 2, works in security in cognitive radio network is reviewed. In Section 3 a new taxonomy of attacks is proposed. In Section 4, a new simulation framework is presented. Results of attacks simulations are shown in section 5. Conclusion and Future Work are offered in Section 6 and 7 respectively.

2 Related work

Most of first publications related with the security field in cognitive radio were developed specifically to analyze the effects produced by characteristics of cognitive radio in the security of the systems and how they could be used to mitigate the negative effects. So in the paper [2] each characteristic and the attacks that could take advantage of it are analyzed. A different point of view is shown in the paper of Zhang and Li [1] .They make a survey about the weaknesses introduced by the nature of cognitive radio. They base the security of the system in two tasks: protection and detection, and divide the attacks and countermeasures depending on which layer of the protocol stack affects. The paper [3] studies threats that affect the ability to learn of cognitive networks and the dynamic spectrum access. To conclude the general references about security, it should be noted the paper of Goerge and Clancy [4] where an attack classification in cognitive networks is done: DSA attacks, Objective function Attacks and Malicious Behavior attacks.

As we discussed above, the spectrum sensing has been one of the most studied areas, even to the point that many of the security papers focus on making sure the sensing task. The idea on which they are based is that security must start ensuring the reliability and truthfulness of the data. The

paper [5] analyzes two specific attacks against cognitive networks: Primary User Emulation, PUE, and sensing data falsification. It also provides some countermeasures well adapted to static scenarios such as TV system. In [6], a secure protocol spectrum sensing is presented. It bases its functionality on the generation and transmission of specific keys to each node. As a third example of safety sensing investigation, the research [7] proposes a collaborative algorithm based on energy detection and weighted combining (similar to a reputation system) to prevent malicious users.

Although previous papers help to understand the importance of safety in this kind of networks they don't focus on any specific attack. The most studied attack against cognitive radio is the primary user emulation, which was defined by Chen and Park [8] for the first time in 2006. Since then much research as the same authors [9] have focused on countermeasures for the effects of the PUE. Also, in the paper [10] shows a way to detect the primary users through an analytical model that does not require location information.

As well as the PUE attack, the community of researchers in cognitive radio has been studying other kind of attacks originate from different wireless networks, such as Denial of Service (DoS) attack or jamming attack. These attacks have special characteristics in cognitive networks, for example, paper [11] studies these features for DoS, and [12] shows a countermeasure based on frequency hopping (technically possible in CR) to avoid jamming attacks.

Summarizing the state of the art, can be draw different conclusions. The first is that there is still much to investigate in the area of security for cognitive radio network, because the works shown are theoretical and they do not cover all the topics that the area provides. The second one, looking the works referenced in this section is that there are not works focused in real scenarios or testbed, as it is proposed in this paper.

3 Taxonomy of attacks

It is imperative to propose a taxonomy of attacks on Cognitive Radio Networks (CRN) to design

optimistic security mechanism. There are several existing taxonomies of the attacks on Wireless Networks [13] and focus on Wireless Sensor Networks [14]. However, there is no a deep classification of attacks in CRN. We have analyzed special network features: maintains awareness of surrounding environment and internal state, adapts to its environment, reasons on observations to adjust adaptation goals, learns from previous experiences, anticipates events in support to future decisions, and collaborates with other devices to make decisions based on collective observations and knowledge. Considering theses features we propose a taxonomy which contains various attacks with respect to different purpose, behavior and target. This will help researchers to better understand the principles of attacks in CRN, and further design more optimistic countermeasures for sensor networks.

Next figure shows an outline of this CRNs taxonomy of attacks.

[FIGURE 1]

Figure 1. Taxonomy of CRN attacks

Communication attacks can be classified in three different types according to the attack behavior: replay attack, Denial of Service attack, and Sybil attack. Replay attack is the replay of messages from inside or outside the current run of communication, message is directed to other than the intended node and intended principal receives message, but message is delayed. This delay is fundamental to calculate network characteristics (channel, topology, routing…). Denial-of-Service attack is characterized by an explicit attempt to present the legitimate use of a service. In this case, services can be the spectrum or a special node. Different kinds of DoS attacks are: jamming attack, the transmission of a radio signal that interferes with the radio frequencies being used by the nodes; collision attack is when an attacker may simply intentionally violate the communication protocol, trying to generate collisions, retransmissions…; Routing ill-directing attack is when a malicious node simply refuses to route messages; and flooding attack is when a malicious node send many

connection request to a susceptible node , rendering the node or the resource useless. Sybil attack is defined as a malicious device illegitimately taking on multiple identities. The Sybil attack is effective against routing algorithms, voting, reputation systems, and foiling misbehavior detection. For instance, the Sybil attack might utilize multiple identities to generate additional reputation to malicious nodes or to change the sensing spectrum information. In Section 4 PUE (Primary User Emulation), a particular kind of Sybil attack, is defined.

The other important attack class is attacks against privacy. CRNs allow sharing resources to establish a communication. For example, a mobile phone could use other device network for an emergency call. Attackers could use this access to take some of node information. The attacks against node privacy include eavesdropping, through taping the information, the attacker could easily discover the communication contents, impersonating attack, where the attacker can insert and it can impersonate the original victim sensor node to receive packet, and traffic analysis, using wireless and cognitive features to listen in the entire spectrum.

Because of the propagation of information node-targeted attacks are very important for CRN works correctly. A node can be captured and attackers use reverse-engineered and become an instrument for mounting counterattacks. Other possibility is to destroy the nodes. This destruction not only affects to node functionality also affects CRN.

The attacker can inflict sleep torture on an energy constrained node by engaging in it in unnecessary communication work to quickly drain its battery power. Depriving the power of a few crucial nodes (e.g. Access Point) may lead communication breakdown of the entire network. Attacker node can request a channel change every time, increasing power consumption.

The security and privacy policy is imperative since the policy basically influences the setup principles of a CRN. Policy attacks can be classified as: excuse attack, if the network policy is overly generous to recovering nodes that recently crashed or damaged by no requiring them to

prove there are maintaining their quota, a malicious node may exploit this attack by repeatedly claiming to have been crashed/damaged; newbie-picking attack, if a CRN require that new nodes pay their dues by requiring them to give information to the net for some period of the time before they can consume any shared resource, therefore a veteran node could move from one newbie node to another, leeching their information without being required to give any information back.

Apart from the above listed attacks that may hinder the key management of CRNs, the following actions will also danger the key management within CRNs: brute forces, dictionary attack, and monitoring attack.

4 Simulation Framework

Once the taxonomy of attacks is done, the next step is to build a simulation framework that allows researchers to simulate attacks and countermeasures. After verifying the simulation results could be made functional prototypes to demonstrate the suitability of simulations to reality.

First project needs open source simulator, indeed we want to have a complete visibility on the source code in order to see how it is working so we can easily modify the code to add CR capacities and validate our modifications. There are many open source simulators, for instance OMNet++ [15], ns-2 [16], WSNet [17], GloMoSim [18], JiST/SWANS [19] and GTNetS [20]. They are all discrete event simulators. OMNet++, ns-2 and GTNetS are general purpose network simulators, whereas GloMoSim, JiST/SWANS and WSNet are more used to simulate wireless networks. We choose ns-2 simulator for several reasons. First, it appeared to be the only one which had a CR add-on (called Cognitive Radio Cognitive Network) already implemented and distributed. Then, it is largely used through the research community so it is quite well documented. Finally, it offers a very large set of protocols and applications.

Ns-2 is not provided with the capacity of doing multichannel simulations. CRCN add-on allows doing multi-MAC interfaces and multi-radio channels simulations. CRCN provide example of a

routing algorithm in the case there are several MAC interfaces and examples of MAC layers which are able to choose the channel they want to use. In the first place, it was only considered the single MAC multichannel because providing devices with multi-MAC interfaces would raise the complexity and prize of the devices. Nevertheless this option could be considered in future works.

The examples of MAC layers provided by CRCN are basic, indeed they are based on contention access with no collisions resolution. Moreover the cognitive capabilities are limited: either it negotiates a communication strategy once at the beginning of the simulation and not does spectrum sensing then, or it checks for PU but not verify then if the PU empty the channel. For those reasons we decided to develop our own MAC layer keeping CRCN as a framework basis.

As we want to be able to simulate either infrastructure-based or adhoc networks, 802.11 MAC layer is one of the best options because it has been largely used to do both. Another advantage is that 802.11 is already implemented in ns-2 so it is not necessary to develop the new CR MAC layer from scratch.

In this case, the nodes will have the ability to choose the channel where it wants to receive packets. Each node will have to send its decision to the other members of the network so they should be able to communicate. This mechanism involves the use of a CCCH on which will be sent the strategy of each node and the information about PU. This channel can be used for exchange security information as well. When a node joins to the network must choose a channel in which it will be able to communicate. In order to do this it will wait for the strategies of the other nodes on the common control channel and then apply the following algorithm: the node searches for a free channel and takes the first it finds, if there is none, the node searches for the channel were there are less other members of the network as possible and chooses that channel. The network is dynamic and conditions can change at any instant, so a node should repeat this process with a variable frequency proportional, for example, to the CCCH capacity. Each node will sense looking for PU in the channel where it is receiving and send an alarm message on the CCCH containing the concerned

channel if it detects one. The sensing can be considered as cooperative because nodes will broadcast the information about detected PUs. Then it updates its strategy and sends it to the others. The nodes will sense all the channels where PU where detected previously in order to check if they are liberated by those PU. A channel can be reelected by a node only if it did not detect any PU packet during at least 10 seconds. We choose this period arbitrarily, it should be set in function of the PU signal characteristics but in our case we define this signal as well. Indeed the PU send (broadcast) packets on a given channel, time and period. In our case we recognize the PU packets with a field in the header of the packet. Indeed the signal is not represented with high accuracy in ns-2 so it is a simple way to characterize PU communications. Those packets are sent every 5 seconds.

The figure below depicts the modified 802.11 diagram state with the classic backoff and RTS/CTS mechanisms and added cognitive features.

[FIGURE 2]

Figure 2. 802.11DSA state diagram

In order to simulate infrastructure-based networks we need to define how the Access Points (AP) or Base Stations (BS) are going to work. We consider that an AP cannot receive on more than one channel simultaneously but it can sense all. So when it detects energy on one channel it will start to receive on this channel, if a new packet comes in the same channel there is a collision, if a new packet comes on another channel it is ignored. When the packet is completely received the AP or BS sense for others on all the channels.

The waveform and access scheme of the CCCH is not defined in the simulator. Nevertheless, an estimation of the amount of data that we need to transmit on this channel would have to be done in the future. We can notice as well that this channel is a weak point of the network so in future studies finding alternatives should be considered.

For our first attack we choose to implement PUE. PUE attacks can be classified in our taxonomy as

Sybil attack that uses only one PU identity. It exists two types of PUE attackers, selfish PUE attackers and malicious PUE attackers. In this section we will describe the behavior we have chosen to give to those two types of attackers.

The goal of a selfish attacker is to empty a channel in order to use it to communicate successfully. So the typical behavior of such a device will be to perform a PUE on a channel, once the channel emptied a new network of accomplice nodes will be able to communicate on this channel. The node that originally performed the PUE then have to regularly send PU packets in order to keep the other devices out of the attacked channel.

The malicious attacker's goal is to prevent the communications of other device by always attacking the channel it chooses. As the information about where the nodes will receive data is broadcasted on the CCCH it is really easy to perform this attack by always performing a PUE on the channel chosen by the target node.

In [8] Chen and Park propose a location-based detection of the PUE attack. This method aims to differentiate an attacker from a PU by checking the origin of the transmission corresponds to the location of the PU. They use two methods for this purpose: one based the power of the signal of the attacker (the Distance Ratio Test, DRT) and the other on the phase of the signal of the attacker (the Distance Difference Test, DDT). Both of these techniques need the introduction of a new type of element in the network named Location Verifier (LV). Those LVs can be either dedicated terminals or integrated in SU terminal. They need to be aware of their location (for instance by embedding a GPS chip) and communicate through a CCCH.

First developed countermeasure implements the DRT in the simulation environment. For this purpose the behavior of LVs has been defined. It is necessary at least two of them in the network, a master and a slave. The slave will measure the RSS of the PU that are detected, calculate its distance from all known PU and send the information to the master through the CCCH. The master

will perform the DRT and see if the PU signal comes from a real PU or from an attacker. We can imagine that the LVs are able to move but the DRT calculation will have to be done with the positions of the LVs at the moment they did the RSS measurement.

5 Results

In this section some of the simulation results and its interpretation will be presented. First network under normal conditions will be simulated and then the effects of the introduction of different types of attacks will be seen. Finally the conclusions are presented.

5.1 Simultation under normal conditions

The goal of this scenario (scenario 1) is to see the effect of the detection of a PU in one of the channels in which the SU were previously transmitting. The input parameters for the simulation are listed below:

- An ad-hoc topology with all the nodes in the communication range of each others.
- 6 nodes involved in communications.
- Rate of communication: 0.5Mbps per transmitting node.
- 3 available channels of 11Mbps.
- Node 1 and 2 are set as PUs emitting from 20s to 90s in channel 3 and from 30s to 90s in channel 2 respectively.
- The duration of the simulation is 100s.

On Figure 3 are represented the percentage of usage of each channel. These measures take into account only SUs' traffic. First, the SUs empty the channels 2 and 3 during the PUs' transmissions. Indeed before the PUs' transmissions begin the three channels are equally loaded. When the first PU

starts its emission, the node that was receiving in channel 3 detects it and decides to receive in channel 2. The usage of channel 2 is doubled. Then the channel 2 is empty by the second PU so all the traffic of the network is supported by channel 1. At the end of PUs' transmissions the load is redistributed between the channels.

[FIGURE 3]

Figure 3. Channel usage of scenario 1

5.2 Network under PUE attack

5.2.1 Selfish PUE

The goal of this scenario is to see the effect of a PUE selfish attack in a very simple network. The input parameters are the following:

- Ad-hoc topology with all the nodes in the communication range of each others.
- 2 available channels of 11Mbps.
- Nodes 1 and 2 are set as selfish attackers which attack channel 2. Node 1 is defined as a PU and emits PU packets on channel 2 at 25.0 s. At 40.0s node 1 starts on channel 2 which destination is node 2.
- 4 nodes involved in communications.
- Transmission rate is 1.5Mbps for SUs.
- Transmission rate of the attackers is 0.5Mbps.
- Duration of the simulation is 100s.

On Figure 4 the percentage of usage of channels 1 and 2 are shown. Until 25.0s the communication of SUs is balanced between channel 1 and 2. At 25.0s the attacker empty channel 2, then all the

communications use channel 1 so the usage is doubled. At 40.0s we see that the attacker's communication begins on channel 2.

[FIGURE 4]

Figure 4. Channel usage of the selfish attack scenario

5.2.2 Malicious PUE

This scenario aims at studying the behavior of the network under a malicious PUE attack.

Taking nearly the same parameters as scenario 1, the only changes are:

- Node 1 and 2 are not PUs.
- Node 1 is a malicious attacker. The attack start at 20.0s and the target is the node 5.

The percentage of usage graphs are shown in Figure 5. All the channels are affected by the attack because the attacked node will change its reception channel every time it detects a PU packet. As previously seen a node has to wait 10 seconds after the last PU packet before it chooses a channel to receive.

[FIGURE 5]

Figure 5. channel usage of the malicious attack scenario

6 Conclusions

This document provides a new taxonomy of cognitive network attacks serving as a reference when it can simulate the consequences that pose different threats to the network. This taxonomy is proposed considering the features of CRN, and is performed depending on different purpose, behavior and target. This new classification will help researches in the area to better understand the security problems and design more optimistic countermeasures.

A Cognitive/DSA MAC layer model is defined and implemented for ns-2 simulator. Although CRCN was providing a good structure it did not permit to simulate a realistic CR/DSA and medium access scheme thus it had to make an effort to adapt the MAC layer.

This work represents an improvement since the simulation effort in the CR field used to be more oriented on PHY layer and spectrum sensing in Matlab. With this new layer, the foundation to have a suitable testbed for CR security simulations is laid. The simulation framework has been tested with a Primary User Emulation attack.

The development based on CRCN/ns-2 and its 802.11 implementation provides an accurate simulation tool for MAC and upper layer. Its conception based on CRCN allows a developer to reuse all the Cognitive/DSA algorithms and apply them in another MAC layer.

7 Future work

Previous sections explained the adaptation of a generic wireless sensor simulator, NS-2, to cognitive radio. The modifications let us to implement different network topologies and some specific tasks of cognitive networks. Even though changes in the NS-2 simulator are designed to implement some attacks and countermeasures, there is a lot of future work to implement.

The immediately future work should be focus on three different aspects: implement a countermeasure against the primary user emulation attack, develop new attacks against cognitive networks and improve the simulator features.

There are many options to implement a countermeasure against PUE, for example, the network could ignore the packets transmitted by the attacker, so the traffic produced by the attacker disappears. Other possible countermeasure is to implement a PUE against the attacker. In this way, the attacker would not take at least all the frequency band. Third option is to do nothing when a primary user emulation attack is detected, that is, the secondary users would continue their

transmissions during the attack. In this case, the noise in the communications is the affected parameter.

Second future investigation line is to develop different attacks over the simulator. PUE is the most characteristic attack in these networks, but as we show in our taxonomy, several attacks have special importance in cognitive radio.

Finally, the third idea of future work try to get the main objective of the project: develop a complete simulation testbed for cognitive radio networks. Developing a complete and accurate simulation is an ambitious project even though we did not start from scratch, but next some modifications are able to be implemented:

- The simulator should be tested with a larger set of input and better packaged parameters before its distribution would be possible.
- Reputation mechanism. Cognitive computing decisions must not be immediate and irrevocable, but much more like human decision it has to be considered and based on experience. Reputation system helps us to identify unusual behaviors which could be attacks.
- Another interesting development should be to implement a CR MAC with a MF-TDMA/DAMA scheme as defined in 802.22 standard in order to simulate more realistic centralized network architecture and perhaps find efficient DAMA configuration.

8 References

[1] Zhang, X. and Li, C. 2009. The security in cognitive radio networks: a survey. In *Proceedings of the 2009 international Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly* (Leipzig, Germany, June 21 - 24, 2009). IWCMC '09. ACM, New York, NY, 309-313

[2] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," CrownCom 2008. 3rd international Conference on, vol., no., pp. 1--7, 15--17 May.

[3] Zhang, Y., Xu, G., and Geng, X. 2008. Security Threats in Cognitive Radio Networks. In *Proceedings of the 2008 10th IEEE international Conference on High Performance Computing and Communications* (September 25 - 27, 2008). HPCC. IEEE Computer Society, Washington, DC, 1036-1041.

[4] T.C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," Proc., Intl. Conf. on Cognitive Radio Oriented Wireless Networks and Commum. (Crown-Com'2008), May 2008.

[5] Ruiliang, C., Jung-Min, P., Hou, Y.T., Reed, J.H.: Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks. IEEE Communications Magazine 46, 50-55 (2008).

[6] G. Jakimoski and K.P. Subbalakshmi, "Towards secure spectrum decision," To appear, IEEE Intl. Conf. on Commun. (ICC'2009), Jun. 2009.

[7] T. Zhao and Y. Zhao, ``A new cooperative detection technique with malicious user suppression," in *Proc. IEEE ICC*, Dresden, Germany, EU, June 2009.

[8] Chen, Ruiliang; Park, Jung-Min; , "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on* , vol., no., pp.110-119, 25-25 Sept. 2006

[9] Ruiliang Chen; Jung-Min Park; Reed, J.H.; , "Defense against Primary User Emulation

Attacks in Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal on* , vol.26, no.1, pp.25-37, Jan. 2008

[10] Jin, Z.; Anand, S.; Subbalakshmi, K.P.; , "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," *Communications, 2009. ICC '09. IEEE International Conference on* , vol., no., pp.1-5, 14-18 June 2009

[11] Brown, Timothy X; Sethi, Amita; , "Potential Cognitive Radio Denial-of-Service Vulnerailities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment," *Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 2nd International Conference on* , vol., no., pp.456-464, 1-3 Aug. 2007

[12] Lei Zhang; Jian Ren; Tongtong Li; , "Spectrally Efficient Anti-Jamming System Design Using Message-Driven Frequency Hopping," *Communications, 2009. ICC '09. IEEE International Conference on* , vol., no., pp.1-5, 14-18 June 2009

[13] Lough, D. L. 2001 *A Taxonomy of Computer Attacks with Applications to Wireless Networks*. Doctoral Thesis. UMI Order Number: AAI3006082., Virginia Polytechnic Institute and State University.

[14] Song Han et al. Taxonomy of Attacks on Wireless Sensor Networks. Proceedings of the First European Conference on Computer Network Defence School of Computing, University of Glamorgan, Wales, UK, 2005.

[15] Varga, A.; , "Using the OMNeT++ discrete event simulation system in education," *Education, IEEE Transactions on* , vol.42, no.4, pp.11 pp., Nov. 1999

[16] Qun, Z.A.; Wang Jun; , "Application of NS2 in Education of Computer Networks," *Advanced Computer Theory and Engineering, 2008. ICACTE '08. International Conference on* , vol., no., pp.368-372, 20-22 Dec. 2008

[17] Helius, G., Fraboulet, A., and Fleury, E. 2007. Worldsens: a fast and accurate development framework for sensor network applications. In *Proceedings of the 2007 ACM Symposium on Applied Computing* (Seoul, Korea, March 11 - 15, 2007). SAC '07. ACM, New York, NY,

222-226.

[18] Zeng, X.; Bagrodia, R.; Gerla, M.; , "GloMoSim: a library for parallel simulation of large-scale wireless networks," *Parallel and Distributed Simulation, 1998. PADS 98. Proceedings. Twelfth Workshop on*, vol., no., pp.154-161, 26-29 May 1998

[19] R. Barr, Z. J. Haas, and R. van Renesse. JiST: Embedding Simulation Time into a Virtual Machine. In EuroSim Congress on Modelling and Simulation, 2004.

[20] Riley, G.F.; , "Large-scale network simulations with GTNetS," *Simulation Conference, 2003. Proceedings of the 2003 Winter* , vol.1, no., pp. 676- 684 Vol.1, 7-10 Dec. 2003

FIGURE 1

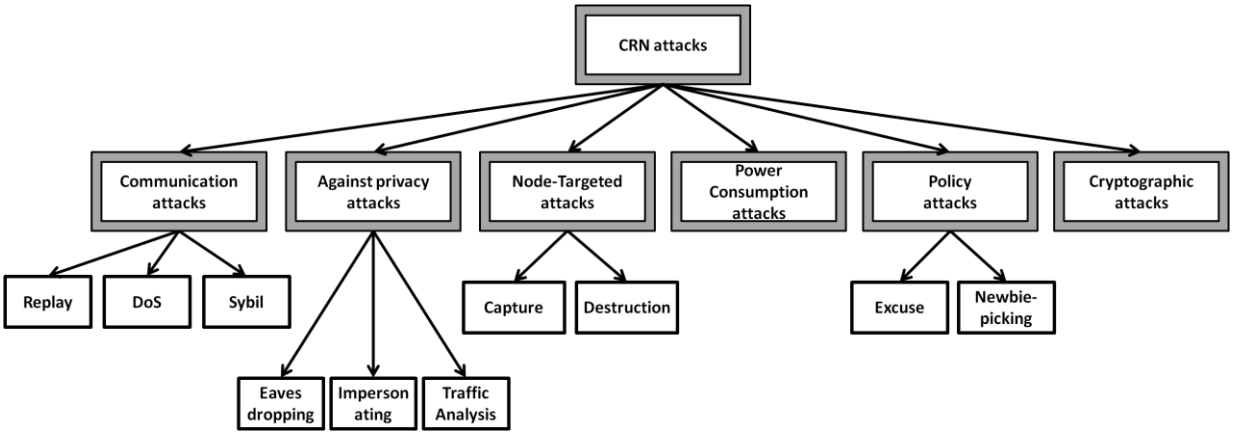

CRN attacks
Communication attacks
Against privacy attacks
Node-Targeted attacks
Power Consumption attacks
Policy attacks
Cryptographic attacks
Replay
DoS
Sybil
Eaves dropping
Imperson ating
Traffic Analysis
Capture
Destruction
Excuse
Newbie-picking

FIGURE 2

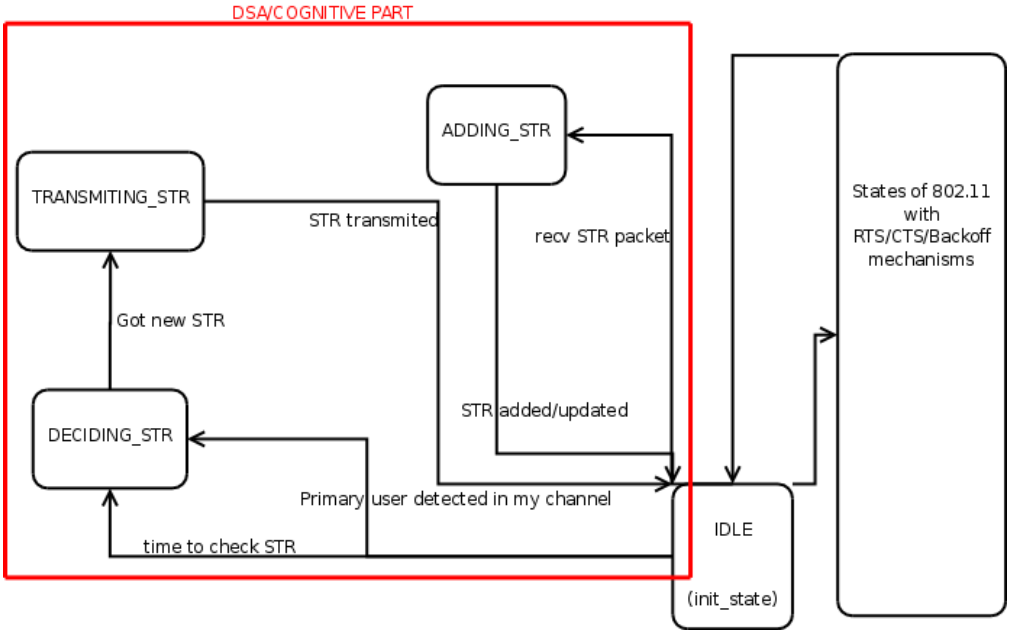

DSA/COGNITIVE PART
ADDING_STR
TRANSMITING_STR
STR transmited
recv STR packet
States of 802.11 with RTS/CTS/Backoff mechanisms
Got new STR
STR added/updated
DECIDING_STR
Primary user detected in my channel
IDLE
(init_state)
time to check STR

FIGURE 3

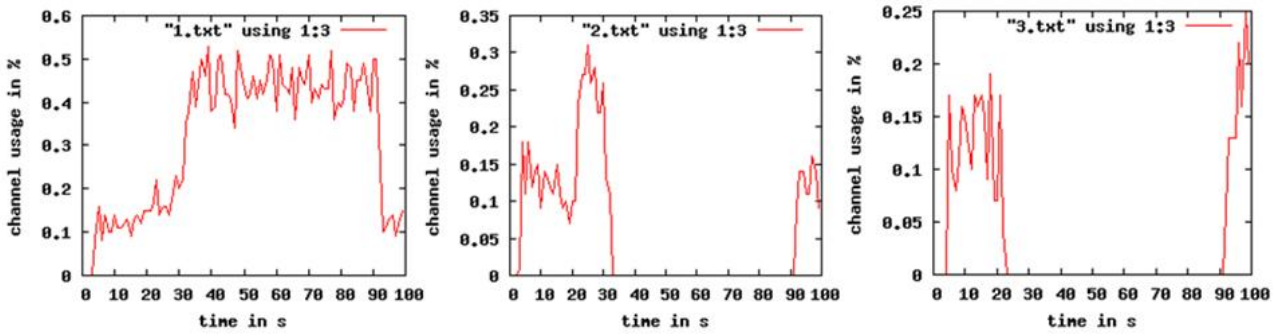

"1.txt" using 1:3
channel usage in %
time in s
0.6
0.5
0.4
0.3
0.2
0.1
0
0 10 20 30 40 50 60 70 80 90 100
"2.txt" using 1:3
channel usage in %
time in s
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0 10 20 30 40 50 60 70 80 90 100
"3.txt" using 1:3
channel usage in %
time in s
0.25
0.2
0.15
0.1
0.05
0
0 10 20 30 40 50 60 70 80 90 100

FIGURE 4

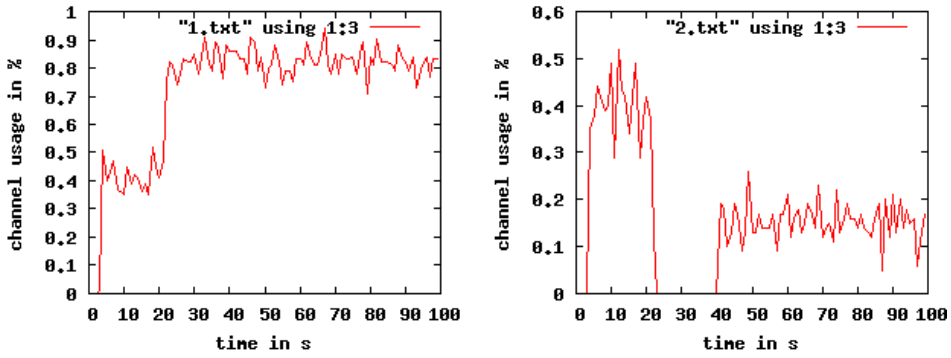
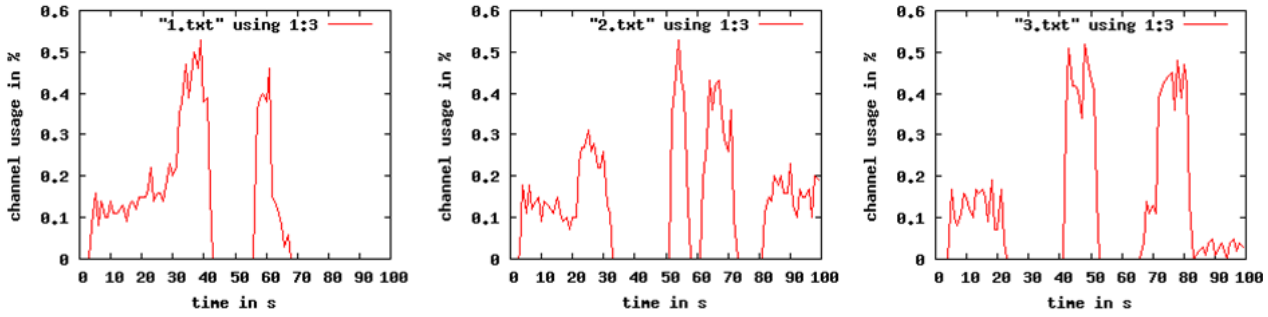

"1.txt" using 1:3
channel usage in %
time in s
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0 10 20 30 40 50 60 70 80 90 100
"2.txt" using 1:3
channel usage in %
time in s
0
0.1
0.2
0.3
0.4
0.5
0.6
0 10 20 30 40 50 60 70 80 90 100

FIGURE 5


"1.txt" using 1:3
"2.txt" using 1:3
"3.txt" using 1:3
channel usage in %
time in s
0.6
0.5
0.4
0.3
0.2
0.1
0
0 10 20 30 40 50 60 70 80 90 100