The Application of Human and Social Behavioral-Inspired Security Models for Self-aware Collaborative Cognitive Radio Networks

Jack L. Burbank and William T.M. Kasch

The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, Maryland 20723
{Jack.Burbank,William.Kasch}@jhuapl.edu

Abstract. This paper discusses the introduction of anthropology and sociology-inspired approaches to providing security in collaborative self-aware cognitive radio networks. This includes the introduction of not only trust models, but also respect models and 'intuition' models. This paper discusses numerous potential benefits from this type of approach, including benefits to algorithm security, compromise recovery, protection from the Byzantine threat, and policy enforcement.

Keywords: Trust model, respect models, collaborative networking, cognitive networking.

1 Introduction

With the ever-increasing need for wireless network capacity and the simultaneous need to increasingly support performance-sensitive multimedia applications, cognitive radios and cognitive radio networking are expected to become an increasingly important part of the overall wireless networking landscape, both in the commercial and military domain. There are currently multiple CR development and standardization activities. One such effort is the DARPA neXt Generation (XG), which aims to develop technology to utilize unused spectrum, primarily for the United States military [1][2]. In the commercial domain, IEEE 802.22 is the primary commercial CR development activity, which aims to develop technologies to utilize unused television spectrum for broadband wireless services [3]. Furthermore, the IEEE Standards Coordination Committee 41 (SCC41), formerly the IEEE P1900 Standards Group, was established in 2005 to develop supporting standards associated with next generation radio and advanced spectrum management.

However, there is an important technical area that has only recently begun to receive serious attention in the cognitive radio paradigm: wireless security. The cognitive radio paradigm introduces entirely new classes of security threats and challenges, and providing strong security may prove to be the most difficult aspect of making cognitive radio a long-term viable concept. This is true in both the military

E. Bertino and J.B.D. Joshi (Eds.): CollaborateCom 2008, LNICST 10, pp. 472–484, 2009.

domain where a deployed network will be potentially subjected to state-sponsored weaponized threats and the commercial domain where the network must protect against both sophisticated and unsophisticated threats. This paper discusses the challenges of providing security in the cognitive radio network paradigm, and discusses the application of a human and social behavior-inspired security framework to these networks to improve overall system security.

2 The Cognitive Network Decision-Making Process

Generally, a cognitive radio exhibits six characteristics [5]:

1. The cognitive radio maintains *awareness* of surrounding and internal state
2. The cognitive radio *adapts* to its environment to meet requirements and goals
3. The cognitive radio uses *reasoning* on ontology and/or observations to adjust adaptation goals
4. The cognitive radio exhibits *learning* from past performance to recognize conditions and enable faster reaction times
5. The cognitive radio *plans* to determine future decisions based on anticipated events
6. The cognitive *collaborates* with other devices to build greater collective observations and knowledge.

Fig. 1 provides a functional decomposition of the general cognitive networking process.

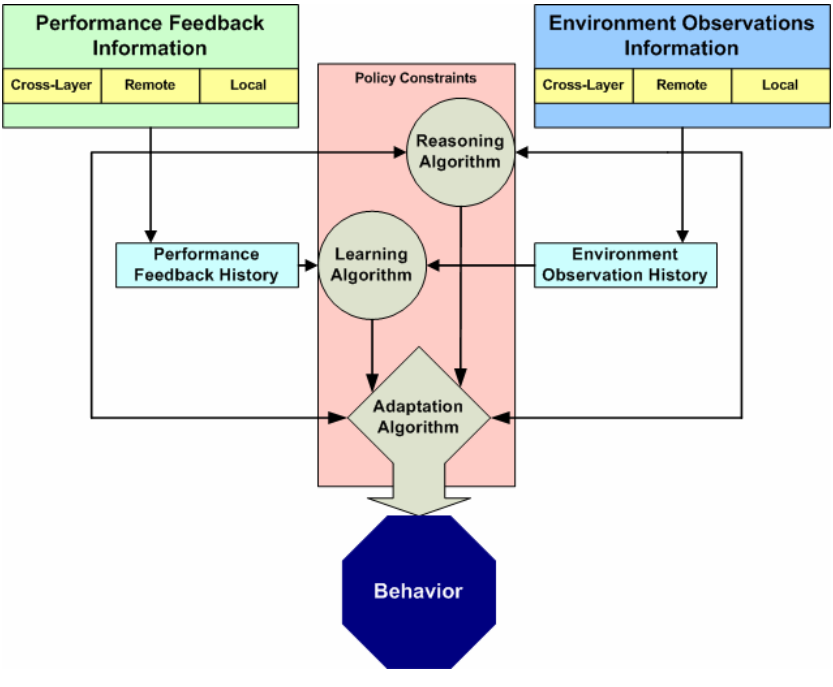

Fig. 1. Generalized Cognitive Radio Decision-Making Process

The cognitive radio maintains *awareness*, which can include observations about its surrounding environment (e.g. spectral density) and observations about its own performance (i.e. error rates). The cognitive radio is *adaptive*, changing some aspect of its behavior based upon observed environment and/or outcome in order to meet its goal (e.g. achieve a certain error rate performance). It should be noted that a radio can maintain awareness without exhibiting any type of adaptivity (e.g. statistics gathering or audit logging for human use). However, these cases are of little interest in the context of this discussion and as such the two functions adaptation and awareness are always co-existent.

It is also important to note that adaptive radios are not necessarily cognitive. There already exist many examples of adaptive radios and techniques that are not considered cognitive [4]. These devices simply adapt based on some pre-defined algorithm or rule-set that does not change over time. Consider the example of adaptive modulation and coding that is based on statically-defined thresholds of link quality. The radio will make some measurement of link quality and adjust its modulation and coding in a pre-defined manner based on pre-defined thresholds. The authors contend that a radio not be considered 'cognitive' unless it employs some degree of *reasoning* and/or *learning*; this position is consistent with that of the larger community.

As shown in the functional decomposition of Fig. 1, reasoning is the function of modifying a radio's adaptation algorithms and rules (which implicitly include objectives and goals) based on current awareness of environment and/or performance in order to best meet the goals of the radio. Algorithms and rules of the cognitive radio are the one and only link back to the goals and requirements of the cognitive radio. Additionally, the function of reasoning might include changing adaptation goals based upon environmental realities.

Learning introduces significant complexity to the cognitive networking paradigm. Now, adaptation algorithms and goals are potentially a function of both current and previous instances of time, up to the maximum history of the learning process (i.e. the amount of time for which external and internal factors influence radio algorithms). The radio notionally keeps track of previously encountered environments, previously attempted behaviors, and previous outcomes to build wisdom of the best decision in given situations. This complexity can dramatically increase the difficulty of understanding and predicting the radio's behavior, creating a significant challenge in forming a stable control system.

Planning is similar to reasoning and learning, except it is making a influencing the adaptation algorithm at a future time. Planning might be based on some history of measured environment or performance. Planning might be the result of a priori knowledge of future events that will affect performance. Planning might be the result of new policy placed into the cognitive network and the cognitive radio wants to provide a smooth transition between old and new policy paradigms.

Collaboration is perhaps one of the easier cognitive functions to understand. Here, the radio is combining its own input functions with the input functions of other radios within the cognitive radio network to form objectives and adaptation criteria. If

reasoning and learning processes are employed, then these composite input functions will affect the basic algorithms of the radio, both current and future.

The general cognitive radio is even more complex, as this type of decision-making process can be taking place at multiple places in the protocol stack and that in fact these layers might be cooperating with each other in a cross-layer approach (depicted by the cross-layer inputs of Fig. 1).

2.1 Cognitive Radio Network Security – A New Complex Dimension of Network Security

There are many aspects of cognitive radio network security that are common to non-cognitive wireless networks, such as the desire to provide user authentication and data confidentiality. But there are many aspects that are unique to the cognitive network that require novel approaches to wireless network security. There are numerous new types of threats to the cognitive network that if not accounted for could enable an entire new class of threats and vulnerabilities [5][6]. To enable further discussion, consider Fig. 2.

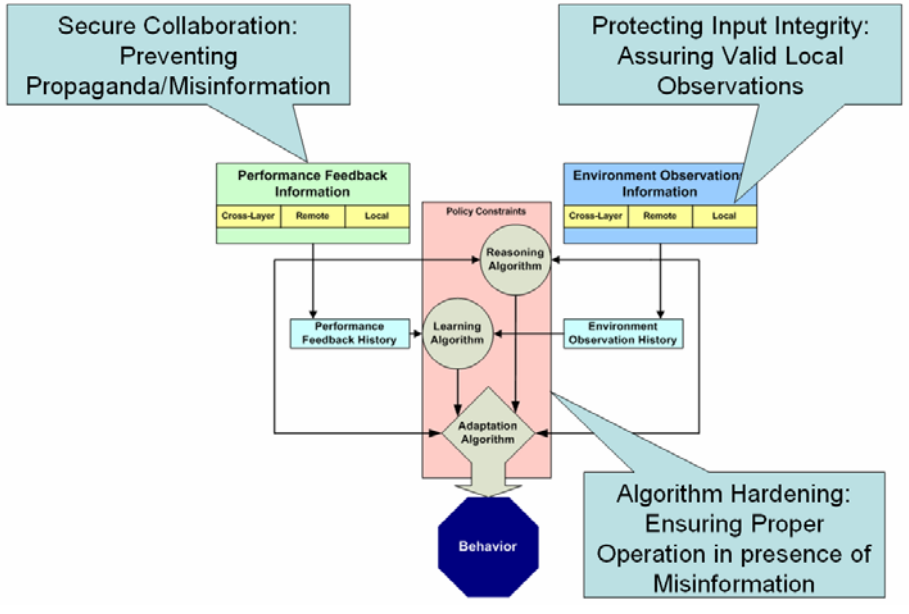

Fig. 2. Required Components of a Cognitive Radio Network Security Architecture

Fig. 3 illustrates the four lines of cognitive network security defense presented in this paper.

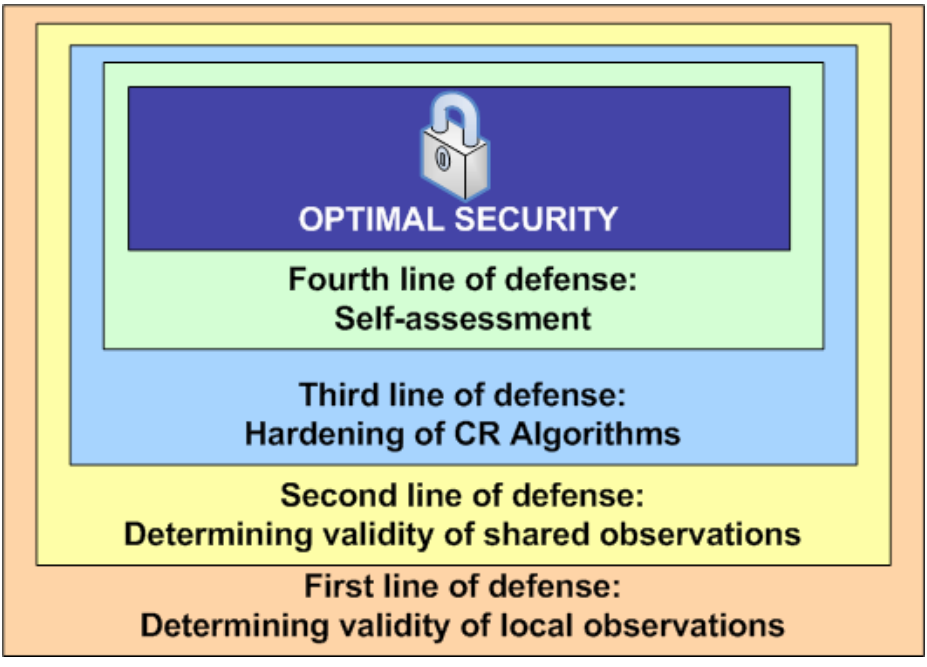

Fig. 3. Cognitive Network Security Lines of Defense

As the first line of defense of the cognitive network, a cognitive radio needs to be capable of judging whether what it is locally sensing is real or falsified. This goes far beyond protecting the network from injection of false messages, as is the focus of traditional network authentication mechanisms. Rather, this means that not only are network messages authenticated, but also that observations of physical phenomena are also authenticated. These physical phenomena include physical attributes of the environment, such as signal presence or channel quality, that do not lend themselves to traditional authentication mechanisms.

Since a CR is utilizing not only its own observations as a basis for decision making but also the observations of others, there is the obvious need to authenticate the shared observations. This is particularly true given the distributed and unseen nature of its peer cognitive radios. Once the authenticity of the source of collaborative CR network messages has been established (which the authors contend is analogous to authentication in traditional non-cognitive networks), the CR needs to be able to judge whether the observations that others within the cognitive radio network are reporting are real or falsified. This, combined with the ability to establish the authenticity of the source, is critical to preventing the propagation of attacker effects within the CR network and is critical for two reasons: 1) to prevent degradation of the greater network because of an individual spoofed cognitive radio element and 2) to protect against the Byzantine (i.e. insider) attack. In this paradigm, the security of each node in the network is dependent upon the security of every other node in the network. This is the second line of cognitive network defense.

Even if mechanisms are put into place to perform authentication of local observations, to perform authentication of collaborative messages, and to determine the validity of remote observations conveyed via collaborative messages, the cognitive radio must still be prepared to properly operate in the presence of malicious information attempting to influence its decision-making process (i.e. the presence of propaganda). This requires that cognitive algorithms be 'hardened' to maximize stability and security (i.e. inability to manipulate or drive the platform into instability because of algorithmic flaws). This includes adaptation algorithms, learning and reasoning algorithms, and planning algorithms. This is the third line of cognitive network defense.

The CR must be able to determine whether it is acting erratically or logically. This self-check is critical to the long-term health of the CR network. If the long-term behavior of the CR has been affected by an attacker, the CR must be capable of identifying itself as an affected node and take self-corrective measures. This aspect is also important because of the envisioned long-term complexity of the CR platform itself. With increasing software complexity, it will be increasingly difficult to test all possible code execution paths to prevent software bugs. Thus, it is important that the CR platform itself is able to perform self-diagnosis to determine if internal problems are present, either because of observation corruption or errors in algorithmic design or implementation. This is the fourth line of cognitive network defense.

Much of the cognitive radio research community is focused primarily on individual problem areas that require maturation. However, as important it is to develop individual protection mechanisms to solve individual portions of the overall problem space, it is equally important to develop an over-arching cognitive network security model to ensure that these individual mechanisms are sufficiently integrated into a single coherent network security approach. This is an area that is receiving little attention in existing research efforts. It is this area in which the remainder of this paper is focused.

3 A Human and Social Behavior Approach

It is important to note that the desired security characteristics previously listed all relate to the need for a cognitive radio to *exhibit good judgment*. It is equally important to recognize that the cognitive radio paradigm imposes human characteristics on the radio device. These radios that now possess human characteristics are then networked together; forming a *virtual cognitive community*, or *virtual cognitive society* and new security threats to this type of network include attempting to manipulate individual networks by influencing the decision-making process. As such, it would appear beneficial to examine social science and human behavior, and consider the characteristics that protect humans from manipulation--primarily relationships, responsibilities, judgment, and wisdom. This is a daunting task, as humanity has not yet mastered these capabilities ourselves. However, it is valuable to consider the human behavioral model in order to isolate protection characteristics that may perhaps be leveraged when beginning to develop a cognitive network security model. Additionally, perhaps the greatest current shortcoming in the area of cognitive radio network security is the lack of a holistic model in which the entire cognitive radio security problem can be viewed, i.e. *a cognitive radio security framework*. This paper

contends that human and social behavioral models have the promise of providing the basis for an effective framework in which to view this problem and to bind individual protection mechanisms into a single coherent system protection approach. This is consistent with human concepts of society and community, and it is likely beneficial to think of a CR network as a virtual community. It should be noted that neuroscience-inspired networking research [9] shows promise, but still remains immature and is largely focused in the area of developing localized optimization algorithms.

Human behavior provides protection mechanisms against deceit in two primary forms: 1) a trust model, and 2) a respect model. How much do we trust the person that is sharing information with us? This trust is typically built over time through experience. There is no 'best' equation as to what this trust versus time model looks like, and often effective human decision making can span a wide variety of these models. But what is consistent in effective collaborative human decision making is the model of 1) friends 2) acquaintances, 3) strangers, and 4) adversaries. This proposed Friend-Acquaintance-Stranger-Adversary (FASA) model in Fig. 4 (which is an expanded version of the Friend-Acquaintance-Adversary model proposed in [5]) aims to leverage a key observation of human behavior: both the trust placed in another individual and the respect placed into another individual's opinion is primarily a function of familiarity, history, and stereotype. Individuals build trust and respect in another individual based, in large part, on how well they know them, previous experiences with that individual, and how trustworthy that individual is perceived to be based upon societal stereotype (e.g. the stigma associated with being a 'used car salesman' or a politician).

However, the last aspect is often individual-unique as biases and prejudices such as these are often taught to them or learned through personal experience; this last aspect is likely to be the hardest to implement in software without unintended consequences. It is also unclear if this aspect is desirable in the cognitive network as these biases can lead

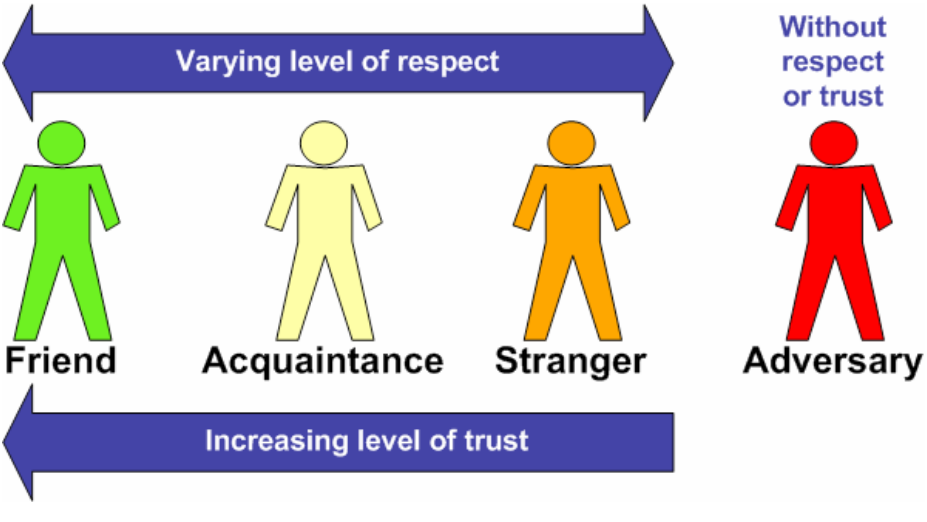

Fig. 4. FASA Model

to poor human decision making. The FASA model is intended to allow the mechanisms to incorporate similar mechanisms into the virtual CR society. Because of factors such as these, the trust an individual is given or the respect that is placed in their opinion can vary greatly across the community population. Another element of the virtual CR society is the law-making body that sets the rules the society must adhere to. In the case of CR, in which policy-based management is envisioned, that law-making body is the CR network designer who develops and configures policies within each CR platform, where each policy can be thought of as a law that must be obeyed.

Friends are elements for which a strong positive trust relationship has been built over time through a deeper level of understanding and familiarity. As such, that understanding can be used to put the conveyed information into a context that can be judged against. The tendency is to trust a friend. Acquaintances are known, but not as well as friends. Here, the tendency tends to remain neutral and not form any type of preconceived notion of trust. Adversaries are the converse of a friend. Here, a deeper level of understanding has been built from which the tendency is to distrust what is being communicated. Strangers are unknown. Here, the tendency generally is to be less trusted. However, the degree of trust placed into strangers can vary greatly across human populations, often influenced by an individual's personal experiences and teachings. Humans achieve this type of understanding over time through gained information, where this information is gained through both direct and indirect communications (i.e. gossip). All of these relationships and the tendency to trust or distrust information are related (at least loosely) to the societal structure and the stated/perceived goals of individuals and individual actions (e.g. custom-based, emotion-based, value-based, etc.). In the cognitive network paradigm, this type of communication represents overhead which is undesirable. So, the goal then is to establish a trust relationship while minimizing the required knowledge to establish the type of peer relationship to be formed with other elements of the cognitive radio network. From a security perspective, it is desirable for a malicious attacker to have as little information as possible to the social values, customs, and motivations of the members of the cognitive radio virtual society. In practical terms, this traces to the need of a malicious attacker to have insight into the goals, methods, and techniques to achieve many of the desired goals (Table 1 from [5]).

3.1 Potential Benefits of a Human-Social Behavioral Approach and Open Research Questions

3.1.1 Trust of Shared Information

Recall the individual CR will eventually make adaptation and perhaps learning decisions based on both locally-collected and remote observations. Thus, the CR platform needs to be capable of judging the validity of observations reported by other CR elements within the CR network. This capability is needed to protect against both the Byzantine threat and the threat of misinformation dissemination amongst the CR network users. This area can take advantage of an overarching model such as the FASA model to determine trustworthiness. Again, there are open research questions that warrant investigation. Should there be designated nodes in the CR network that primarily assess the reasonability of shared observations in an attempt to protect nodes (perhaps a subset) of the network?

Given a set of situational awareness data and desired goals, the algorithms present in the cognitive radio will attempt to make the best decision that will come closest to meeting the set of desired goals. Trust and respect models, such as those enabled by a FASA model, could be employed to police the set of input data that is fed into the decision-making process to provide a line of defense for the algorithms themselves. For example, information that is known to be falsified can be removed from the decision-making process. Information that is more reliable than other information can be weighted differently to have more profound impacts on the decision-making algorithms. It is here that it is believed that behavioral models can be employed to assist in cognitive decision making.

3.1.2 Health and Diagnosis

The CR needs to be able to judge whether it is acting erratically or logically. This self-check is critical to the long-term health of the CR network. At the individual level, humans are typically quite poor at this type of self-diagnostic in an isolated manner. Rather, humans often require communications and interactions with other humans, such as friends ('Is everything OK?') for initial identification of an issue. And even following initial identification, humans often struggle to correct undesired behavior without intervention from friends or paid professionals (e.g. therapists). Reliable isolated self diagnosis may prove difficult to accomplish (if a cognitive radio's algorithms have been compromised how much assurance can be placed that its self-diagnosis functionality is still trustworthy?) and that a distributed approach should instead be considered. Furthermore, a standalone approach may not be desirable because any self-diagnosis function would have to have ultimate access to the rest of the cognitive radio, which could in itself be dangerous.

A FASA model could work well in the CR paradigm to facilitate distributed health diagnosis functions. However, there are numerous ways in which this could potentially be accomplished. Perhaps the cognitive network society is 'friendly and nurturing' and every node helps care for not only itself but for other nodes within the CR network. Or perhaps a 'self-centered' cognitive network approach could be employed, where nodes are not particularly concerned about the health of its neighbors until suspected problems of its neighbors are suspected to be interfering with their own performance. Additionally, the CR could follow the human model even further and have a subset of CR nodes identified as network diagnostic nodes (i.e. therapists) that are charged with analyzing behavior of CR network nodes and assessing the presence of erratic behavior and then assist in the resolution of these issues. Yet another approach would be to assign a subset of CR nodes with the responsibility of policing the CR network, performing assessment of CR node behavior. An approach could also incorporate some combination of all these models. Distributed health diagnosis is a topic that warrants additional research to determine its viability and to assess the strengths and weaknesses of possible approaches.

3.1.3 Byzantine Protection

The Byzantine attack represents the case where a friend or acquaintance has, unbeknownst to the greater cognitive radio network, become an adversary and represents the most difficult subset of this problem space. The Byzantine threat could be substantially more problematic in a collaborative cognitive network. Here, the

compromised node can spoof data to its neighbors in an attempt to destabilize or otherwise control or influence learning and reasoning algorithms. Furthermore, the adversary now has potential access to cognitive algorithm software implementations that could perhaps be leveraged into advanced exploits against the cognitive network. Furthermore, the adversary now has potential access to a rich set of network state information that may be useful in further attacks. There are indeed lessons that can be drawn from existing work in the area of Byzantine routing (e.g. [8]). However, we must be careful not to create an overly-paranoid network where nodes are quickly distrusted if behavior of friends or acquaintances becomes inconsistent with expectations. This paranoia itself could be used against the cognitive radio by an attacker to cause a forced effect. In the case of a cognitive radio employing a FASA model, a friend node is likely easier to identify as a Byzantine threat than an acquaintance or stranger. The application of the behavior models for the purposes of Byzantine protection warrants additional research.

3.1.4 Hostility Characterization

In the majority of cognitive networking discussions, the radio is attempting to perceive one or more aspects of its environment. However, there are generally little existing discussions related to building a view of the safety of the environment. Is a particular node currently under attack by a threat? Is the cognitive network operating in an environment known to be hostile? What is the history of hostile acts taken against the network as a whole? Building this type of view of the environment, and sharing this information throughout the cognitive network, could help build context that could potentially be integrated into trust and respect of collaborative information, belief in authenticity of locally-observed environment, and in the hardening of decision-making algorithms by introducing the concept of 'caution' or 'degree of alertness' based on perceived safety of environment. Returning to the human behavioral model, this is analogous to an individual or group of individuals altering behavior based on comfort and perceived personal safety.

3.1.5 The Role of Others in Localized Decision-Making

While this appears a promising model to follow in the cognitive networking paradigm, there are many unanswered questions. In human society, there are individuals designated to enforce the rules of society (i.e. police). Is it beneficial to appoint a subset of cognitive network nodes as the 'police' of the network, to ensure that the policies of the network are being followed? In human society, a large set of human behavior is affected by teachings (parents, teachers, mentors, role-models, etc.). Is it beneficial to have a subset of the cognitive network population act in similar roles?

3.1.6 Non-direct Trust and Respect

In human society, the attitudes individuals develop towards other individuals are formed not only by direct interaction but also from indirectly received information, which may be completely accurate or not. Would this type of 'gossip' prove beneficial to the security of a cognitive network in building trust in members of the cognitive network community? In many cases, humans rely on intangible 'gut instinct' in placing trust and respect in other individuals (e.g. an individual trusts one

stronger but distrusts another stranger for no apparent reason). This type of factor could be introduced through an 'intuitive model' where decisions are randomized in some fashion so that behavior is not perfectly deterministic. Here, the degree of importance placed on the 'intuitive' factor would be a function of accumulated wisdom (i.e. cognitive radios learn to either trust or distrust their 'gut instinct' much the same way humans do). Is this type of behavior beneficial in the cognitive network society? Questions such as these, as well as many others, should be addressed as this type of model is explored and matured to assess the viability of this model.

3.1.7 How to Develop Respect

From these research communities there is significant work that can be leveraged to begin developing security solutions for CR networks. For example, researchers have considered the issue of optimally combining advice from a set of experts (e.g. [7]), analogous to CRs sharing their expert advice regarding their environment, and several solutions have been proposed that attempts to optimally combine those expert opinions in a way that is most beneficial (e.g. [7]). However, this begs the question which CRs in a community are considered "experts" as well as "trustworthy?" Perhaps this definition of "expert" is governed by policy loaded into the CR. However, this approach is questionable as cognitive networks will likely accumulate knowledge at non-identical rates. Another approach is to build the ability into a CR to determine who it considers an "expert" as well as building the mechanisms into the cognitive network to enable such determinations. This could be enabled by the respect models of the FASA model. Additionally, perhaps this process of determining "experts" is not done individually but rather nodes build "reputations" in the network and the network as a whole gravitates towards decisions regarding who are "experts" and who are not.

3.1.8 Micro versus Macro Behavior

In human and social behavioral models there is a limit to the number of complex relationships an individual can maintain. Dunbar, an English anthropologist, theorized that there is a limit to human cognitive capacity that limits the number of stable social relationships that can be maintained by a human. This led to Dunbar's Rule of 150 (rounded from 148), which states that the mean group size that can be achieved while maintaining social stability is 148. As a community increases in size, an increasing amount of effort is required in 'social grooming' activities to maintain social cohesion and maintain social and cognitive stability. For groups larger than this, behavior must be restricted through rules and laws to maintain social stability. Furthermore, as the number increases, a hierarchy is generally required where smaller groups of intimate groups are formed with less knowledge of other groups.

It is an intriguing research question as to whether this same type of dynamic holds for the cognitive radio network, as this would have numerous ramifications: 1) it places another dimension on network scalability, cognitive capacity, 2) it places bounds and limits on the way the network is governed (micro vs. macro behavior), and 3) it suggests that hierarchy with differing types of relationships among different groups and levels of that hierarchy will be required for large cognitive networks.

Also of interest is the effect of the decision making process, both from a short-term and long-term perspective. For instance, human models show that decisions often

have both short- and long-term consequences—a clear example of this is making the decision to attend college. Generally, those who attend college are sacrificing short-term economic gains and increasing their own short-term workload in order to achieve more desirable, longer-term goals, such as financial security and career stability. One could argue that these longer-term goals provide an increase in the overall "health" of society, which seems like a very reasonable long-term goal for any society to maintain. Cognitive network members and societies may tend toward short-term or long-term goals, and as such, may need to strike a balance in the decision making process, both individually and collectively. More research is warranted in this area to determine the effects of the decision making process on both short- and long-term consequences.

4 Conclusions

This paper proposes that since the cognitive radio paradigm imposes human characteristics on radios that it is appropriate to consider human and social models when considering how to build and protect cognitive networks. This paper contends that there may be valuable lessons from the fields of anthropology and sociology that can be applied to designing secure cognitive networks. Bio-inspired techniques are being applied to the field of cognitive radio, but typically focus on algorithm development rather than considering the macro-level network. This paper does not propose definitive solutions, nor does it benchmark potential solutions. The authors believe that providing security in the cognitive network paradigm may likely prove to be an NP-Complete problem, similar to optimizations in the traditional knapsack problem in a variety of dimensions (time, space, frequency, and power are primary examples). As such, extensive research is certainly necessary before moderately successful solutions emerge. This is believed to be particularly true in the case of an over-arching framework that can bring individual security mechanisms together into a cohesive solution that can enable secure collaborative cognitive networks. Rather, this paper proposes these concepts in hopes that the greater research community will consider these alternate fields of research as sources that can be leveraged.

The authors plan to continue maturing these concepts and to begin implementation of these types of approaches in the form of both modeling and simulation (M&S) and in a Software-Defined Radio (SDR) testbed environment in order to begin answering many of the research questions posed in this paper.

References

1. The XG Vision, Request for Comments, Version 2.0, XG Working Group, http://www.darpa.mil/ato/programs/XG/rfcs.htm
2. The XG Architectural Framework, Request for Comments, Version 2.0, XG Working Group, http://www.darpa.mil/ato/programs/XG/rfcs.htm
3. Cordeiro, C., et al.: IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios. In: 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), November 8-11, pp. 328–337 (2005)

4. Goldsmith, A.J., Wicker, S.B.: Design Challenges for Energy-Constrained Ad Hoc Wireless Networks. IEEE Wireless Communications Magazine (August 2002)
5. Burbank, J.L.: Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security. In: Proceedings of the Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), May 15-17 (2008)
6. Burbank, J.L., Roger Hammons Jr., A., Jones, S.D.: A Common Lexicon and Design Issues Surrounding Cognitive Radio Networks Operating in the Presence of Jamming. Accepted for presentation at the 2008 IEEE Military Communications (MILCOM) Conference (November 2008)
7. Cesa-Bianchi, N., et al.: How to use Expert Advice. Journal of the ACM (May 1997)
8. Awerbuch, B., Holmer, D., Nita-Rotaru, C., Rubens, H.: An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In: ACM Workshop on Wireless Security (WiSe), September 28 (2002)
9. Reggia, J.A., Sutton III, G.G.: Self-processing networks and their biomedical implications. Proceedings of the IEEE (June 1988)