INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A MEANFIELD APPROACH FOR SECURITY ENHANCEMENT USING CR NETWORK

[1]Prasanna.K, [2]Vijayalakshmi.R, [3]RajaPriyanga.C, [4]Shunmugapriya.T

[1]BE (CSE), ULTRA college of Engineering, Madurai, India
[2]BE (CSE), ULTRA college of Engineering, Madurai, India
[3]BE (CSE), ULTRA college of Engineering, Madurai, India
[4]Assisstant Professor, ULTRA college of Engineering, Madurai, India

Abstract: - Cognitive radios are fully programmable wireless devices that can sense their environment and dynamically adapt their waveform, channel access type, spectrum usage, and network protocols which are needs for network and application performance. Using recent advances in mean field game theory, a novel game theoretic approach with multiple players for security in CR is proposed. The mean field game theory provides a powerful mathematical tool for problems with a large number of players .Cognitive radios hopes to improve spectral utilization by allowing users from crowded bands to bleed off into empty bands nearby. Every node in the present scheme needs to know its own state information and the aggregate effect of the other nodes in fully distributed scheme. Since the proposed scheme is distributed in nature it has the capability to prevent Distributed DoS as well. DoS attacks consume the resources of a remote host or network that would otherwise be used for serving legitimate users. The performance of the proposed algorithm in a series of simulations reveal that the proposed scheme provides a better solution than existing approaches with no extra overhead.

Keywords*:* Cognitive radio, peer to peer, DoS, security, CR network.

1. Introduction

Cognitive radios offer the promise of being a disruptive technology innovation that will enable the future wireless world. The cognitive radio technology will soon emerge from early stage laboratory trials and vertical applications to become a general-purpose programmable radio that will serve as a universal platform developing a system for wireless, name as microprocessors acts a similar role for computation [1]. There is however a big gap between having a cognitive radio which is more flexible, supporting building block, and the large-scale deployment of cognitive radio networks that dynamically optimize spectrum use.

Building and deploying a network of cognitive radios is a complex task [2]. There is a growing concern that proceeds with conventional academic research in this area has reached a point of diminishing returns and that further progress in the above areas will depend on a new approach involving multi-institutional research teams working with real-world experimental deployments of cognitive radio networks.

Cognitive radio will lead to a revolution in wireless communication with significant impacts on technology as well as regulation of spectrum usage to overcome existing barriers [3]. Cognitive radio, including SDR as enabling technology, is suggested for the first time in to realize a flexible and efficient usage of spectrum. CR

is an uplift of SR combined from SDR. This cognitive radio is the consequent step from a flexible physical layer to a flexible system as a whole similar to reconfigurable radio. The term cognitive radio is derived from "cognition".

The cognitive radio is a aware communication system that uses spectrum intelligently which coordinates usage of spectrum. It also involves regulation and assigned communication [4]. This secondary usage of spectrum is referred to as vertical spectrum sharing, which is introduced. To enable transparency to the consumer, cognitive radios provide besides cognition in radio resource management also cognition in services and applications [5]. The mental processes of a cognitive radio based on the cognition circle from are depicted Cognition is illustrated at the example of flexible radio spectrum usage and the consideration of users preference. In observing the environment, the cognitive radio decides about its action. An initial switching on may lead to an immediate action, while usual operation implies a decision making based on learning from observation history and the consideration of the actual state of the environment.

2. Providing Security Through COGNITIVE RADIOs

The issue of spectrum underutilization in wireless communication can be solved in a better way using Cognitive radio (CR) technology [6]. Cognitive radios are designed in order to provide highly reliable communication for all users, that how much needed and to facilitate effective utilization of the radio spectrum. To relatively low utilization of the licensed spectrum, is large due to inefficient fixed frequency allocations than any physical shortage of spectrum. This observation has forced the regulatory bodies to search a method where secondary (unlicensed) systems are allowed to opportunistically utilize the unused primary (licensed) bands commonly referred to as white spaces [7]. Cognitive radio can change its transmitter parameters based on interaction with environment in which it operates.

Cognitive radio includes four main functional blocks: spectrum sensing, management, sharing and mobility. Radio Identification Based Sensing a complete knowledge about the spectrum characteristics can be obtained by identifying the transmission technologies used by primary users [8]. Such identification enables cognitive radio with a high dimensional knowledge and also high accuracy.

a) Usage of CR protocol for ad-hoc network provision

The propose of a MAC protocols for cognitive radio wireless ad-hoc, collision free and guaranteeing fair channel assignments. A distributed CR routing protocol for ad-hoc networks is proposed that makes the following contribution [9]. Explicit protection for PU receivers that are generally not detected during spectrum sensing, allowing multiple classes of routes based on service differentiation in CR networks. It affords Scalable, joint route spectrum selection. The route setup in CRP follows two stages in which each CR users identify best spectrum point. Initiative is mapped to delay function for forwarding the required RREQ message.

b) Peer to Peer Communication based on Mobile Ad Hoc Networks

Basic features of mobile ad hoc networks includes Open and unreliable transmission medium, Data are easily disclosed to unwanted third parties Node mobility and constantly changing topology, Data communication may be rattled, infrastructure Selfish nodes refuse to forward packets for other because System performance may severely downgraded, Limited power supply for each node Consequence: SHORT transmission range and limited computation capability [10]. Most of existing works on applying game theories to security only consider two players in the security game model: an attacker and a defender. Distributed algorithms have been studied to determine the networking organization, routing, and link scheduling. IDS can detect the attack with a probability depends according to its received messages.

Bayesian game is implemented to study the interaction between the legitimate nodes and the malicious nodes. Peer to Peer communication is been implemented. Enlarged network is not possible. MANET is infrastructure less network. So, security reduces for large network. They have no centralized administration. It is not possible in MANET. Each major player has a minor player. Some defect that occurs listed [11]. System offers multiple attackers often use the system but there is no strong defensive mechanism. Multiple attackers but not offers multiple defenders to protect against the attackers since it doesn't provide trusted system. It does not offer enough flexibility to compose applications and policies. Cost function and error estimate is complexity for major and minor players and also uses energy and decreases network lifetime. Cost of energy is inefficient.

c) Performance of MANET with limited energy

We consider the network lifetime with two constraints. The first constraint is that if on node's energy consumption reaches 90%, the node cannot work well. When there are more than 70% nodes in the MANET that cannot work well, the MANET will be considered dead [12]. The second constraint is that if the node's loss of security value reaches 80%, the node is compromised. The network is deemed compromised when there are more than 50% nodes in the MANET compromised. We assume that each node has the same initial value of the combination of energy and security.

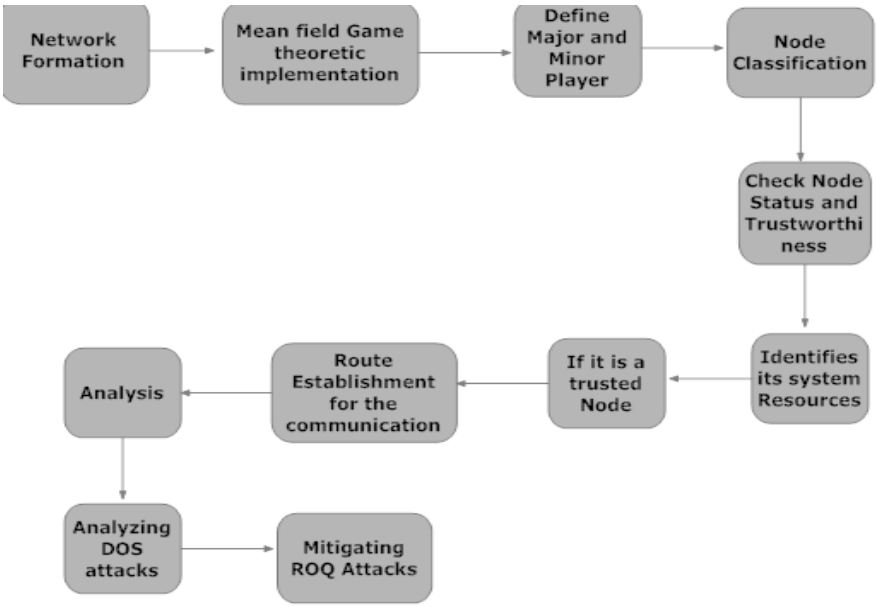


Figure.1. Mitigation Cognititive Radio Network

Basic features of cognitive radio includes Open and unreliable transmission medium, Data are easily disclosed to unwanted third parties Node mobility and constantly changing topology, Data communication may be frequently disrupted, Absence of pre-deployed infrastructure Selfish nodes refuse to forward packets for others because System performance may severely downgraded, Limited power supply for each node Consequence: SHORT transmission range and LIMITED computation capability. Game theory can provide a useful tool to study the security problem in cognitive radio (CR). Most of existing works on applying game theories to security only consider two players in the security game model: an attacker and a defender. In this system proposed a novel game theoretic approach with multiple players for security in COGNITIVE RADIOs. Proposed scheme is fully distributed that can enable an individual node in COGNITIVE RADIOs to make strategic security defence decisions without centralized administration. Proposed scheme considers not only the security requirement of COGNITIVE RADIOs but also the system resources. Proposed scheme scenario offers multiple attackers and multiple defenders. It is also interesting to consider MANETs with cognitive radios.
Both security requirement and system resources were considered in proposed scheme.CR protocol is used to implement the MANET nodes. Mean field approximation approach .Dynamic programming approach is used. AODV is used as routing protocol to reduce traffic with existing links. Enable the deployment of secure applications in the CR networks by the integrated check constraints.

Algorithm Explanation

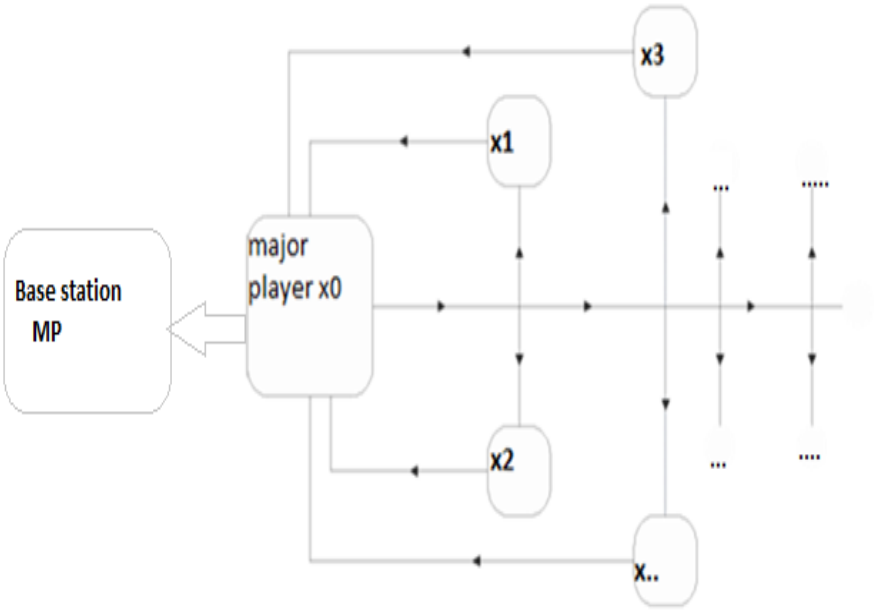
1) Mean Field Approximation:

By using the mean field approximation approach for overcoming the fundamental complexity difficulty, the mean field Equation system can be given as follows:

$\theta(t+1) = \phi(x0(t), \theta(t))$, (6)

$V(x0, \theta) = \min$

$u0 \in A0$
$\{c0\ (x0, u0, \theta) + \Delta\}$,(7)
$W\ (xi, x0, \theta) = \min$
$ui \in A$
$\{C\ (xi, ui, x0, \theta) + \Omega\}$, (8)



Where $\Delta = \rho \sum_{k \pounds s0}$
$Q0\ (k\ |x0, u0)$ v $(k, \phi(x0, \theta))$ and
$\Omega = \rho \sum_{i \pounds s\ k \pounds s0}$ _ $Q\ (j\ |xi, ui)\ Q0\ (k\ |x0, \hat{}\pi 0)$ w $(j, k, \phi\ (x0, \theta))$. $\theta\ (t)$
Presents a limiting process, which is used to approximate the random measure process $I(N)$ (t) for a low complexity Solution.

2) The cost function of the major player

$c0(x0, u0, \theta) = f0\ (x0, u0) - \theta 0$
N
I=1
$(1 - \gamma)\ \beta i$,

d) Network Formation

In proposed the defender identify the attacker and compromises its mean value and become a defender.
Proposed system considered as an N +1 mean field game model as follows. The information is often fragmented, as itself becoming more and more minified in available shorter time frames.

- CR protocol- procedure of getting something through the connection something else.
- In proposed more radical implementation of CR protocol which may turn to the generalized approach.
- Enable adaptive approach in utilizing existing wireless spectrum.

Consider the defending cognitive radio nodes as the N minor players. Meanwhile, the attacker, which tries to attack the CR, is considered as a major player $A0$. Cognitive radio networks are formed to show the interactions between the major player and the minor player.

3. Mean Field Game Theoretic Implementation

The interactions between the major player (as an attacker) and a representative minor player (as a defender) are modelled as a non-cooperative non-zero-sum game. Mean field approximation approach is used for overcoming the fundamental complexity difficulty. Dynamic programming approach is used. Using the dynamic programming method, obtain the major player's optimal strategy $\pi 0$ by the dynamic programming. With the pursued $\pi 0$, the representative minor player's optimal strategy π can also be acquired. Nodes are classified using the mean field equations. Major and minor player states are obtained using the mean field equation. Defenders states are also obtained. Beacon message is used.

Error Analyzing and Estimation

Mean field approximation equation is used for the examination of the system performance by calculating error estimation. Analyze the node behaviour over the total amount of packets that the node has received such as packet drop rate (PDR), packet modification rate (PMR) and RTS flooding rate. In classification phase, analyze the node density, Radio range, Adversary percentage, node mobility for calculating the node trust value. Performance of the system can be evaluated by calculating the correctness and efficiency of the SAT scheme: Precision, Recall, Communication overhead (CO), and Convergence Time.

4. Conclusion

The ability of terminals and network segments to seamlessly adapt to changes in the radio environment will be provided through the mechanisms offered by the reconfigure concept. Moreover, with the use of reconfigurable technologies, more flexible network architecture can be achieved and programmable network management can be carried out. In the future, network management functions should not only consider the features and capabilities of the actual network elements, but should also include traffic demand, resource and traffic scalability, as well as the cooperation between different networks to efficiently allocate the overall available resources. It is anticipated that, due to the self tuning approach, system performance can be significantly improved. This in turn will help to reduce the deployment and operational cost of networks.

REFERENCES

[1] Yanwei Wang ,F. Richard Yu, "A Mean Field Game Theoretic Approach for Security enhancement in Mobile ad hoc networks," *IEEE Security Privacy, vol. 6, no. 2, pp. 72–75, Mar. 2014.*
[2] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, pp. 188–190, July 2013.
[3] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2674– 2685, July 2012.
[4] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 806–815, Feb. 2009.
[5] M. Carvalho, "Security in mobile ad hoc networks," *IEEE Security Privacy*, vol. 6, no. 2, pp. 72–75, Mar. 2008.
[6] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in *Proc. 2000 ACM MOBICOM*, pp. 275–283.
[7] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–60, Feb. 2004.
[8] T. Alpcan and T. Basar, *Network Security: A Decision and Game Theoretic Approach.* Cambridge University Press, 2010.
[9] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 2013.
[10] H. Bedi, S. Roy, and S. Shiva, "Game theory-based defense mechanisms against ddos attacks on TCP/TCP-friendly flows," in *Proc. 2011Computational Intelligence Cyber Security*, pp. 129–136.
[11] A. Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," *Int'l J. Netw. Security*, vol. 2, no. 2, pp. 131–137, 2006.
[12] E. A. Panaousis and C. Politis, "A game theoretic approach for securing AODV in emergency mobile ad hoc networks," in *Proc. 2009 IEEE Conf. Local Comput. Netw.*, vol. 53, pp. 985–992.

[13] J. Omic, A. Orda, and P. Van Mieghem, "Protecting against network infections: a game theoretic perspective," in *Proc. 2009 IEEE INFOCOM*, pp. 1485–1493.
[14] N. Santosh, R. Saranyan, K. Senthil, and V. Vetriselvi, "Cluster based cooperative game theory approach for intrusion detection in mobile ad-hoc grid," in *Proc. 2008 International Conf. Advanced Comput. Commun.*, pp. 273–278

Prasanna.K, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

Vijayalakshmi.R, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

RajaPriyanga.C currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

Shunmugapriya.T, completed her B.E(CSE) in Pandian saraswathy College of Engineering and Technology(2009) M.E(CSE) in Raja college of Engineering and Technology(2011) M.B.A(systems) Madurai Kamaraj University(2013) Lecturer on CSE DEPT 4YEARS EXPERIENCE, is currently working as an Asst Prof. in Ultra College of Engineering & Technology for Women, Madurai.