IJournals: International Journal of Software & Hardware Research in Engineering
ISSN-2347-4890
Volume 3 Issue 6 June, 2015

Cyber Security Forecasting in Wireless Networks using Game-Theoretic Approach

Author: Khyati Chopra[1] ; Ranjan Bose[2]

Affiliation: [1](Electrical Department, IITD, Delhi, India
Email: [1](eez148071@ee.iitd.ac.in)

***Abstract*—Recently, wireless networking for emerging cyber-physical systems, in particular the smart grid, has been drawing increasing attention and hence risk of secure transmission of information or message has increased. In wireless sensor network, due to nature of broadcast communication there is possibility of eavesdropping, interception and alteration or modification of message. Thus, protecting this communication channel from malicious attacks is an important yet challenging security issue in mobile networks. With energy constraints for both the defender and the attacker, the interactive decision making process of when to send benevolent data signals and when to attack through fraudulent jamming signals has to be understood. In this paper, the objective is to consider the most reputable communication path in wireless networks from the game-theoretic viewpoint and therefore provide the optimal strategies to constitute Nash equilibrium and hence improve the network throughput greatly. Also, we analyze mixed strategy channel selection algorithm to maximize the utility of each player.**

Keywords: Cyber-Physical Systems, game theory, Nash Equilibrium, security

I. INTRODUCTION

THE advancement of today's wireless technologies (e.g., 3G/4G and WiFi) has already brought significant change and benefit to people's life, such as ubiquitous wireless Internet access, mobile messaging and gaming. On the other hand, it also enables a new line of applications for emerging cyber-physical systems (See Fig.1), in particular for the smart grid where wireless networks have been proposed for efficient message delivery in electric power infrastructures to facilitate a variety of intelligent mechanisms, such as dynamic energy management, relay protection and demand response. The cognitive network (CN) users are equipped with cognitive radio devices, which enable them to perform various dynamic spectrum access techniques including spectrum sensing, seamless handoff, spectrum management, and spectrum sharing [1]. INTERNET of Things (IoT) has been emerging as the next big thing in Internet. It is envisioned that billions of physical things or objects will be outfitted with different kinds of sensors and actuators and connected to the Internet via heterogeneous access networks enabled by technologies such as embedded sensing and actuating, radio frequency identification (RFID), wireless sensor networks, real-time and semantic web services, etc. IoT is actually cyber-physical systems or a network of networks. With the huge number of things/objects and sensors/actuators connected to the Internet, a massive and in some cases real-time data flow will be automatically produced by connected things and sensors. It is important to collect correct raw data in an efficient way; but more important is to analyze and mine the raw data to abstract more valuable information such as correlations among things and services to provide web of things or Internet of services.

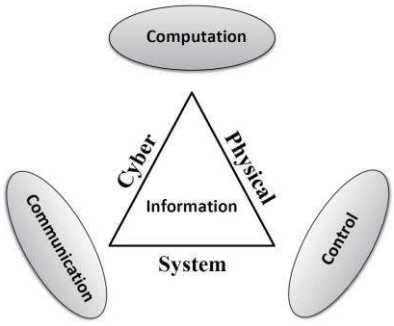

Fig.1: Architecture of Cyber-Physical Systems

Security is a broadly used term encircling the features of authentication, non repudiation, privacy, integrity and anti-playback**.** An important, yet open research question is how to model and detect jamming attacks in wireless system, such as cellular and WiFi networks [2]-[5]. Different detection strategies have to be studied to find the probability of false alarm and the probability of missed detection. Based on an information-theoretic formulation of the problem, in which two legitimates

partners communicate over a quasi-static fading channel and an eavesdropper observes their transmissions through a second independent quasi-static fading channel, the important role of fading is characterized in terms of average secure communication rates and outage probability.

Wireless networking for emerging cyber-physical systems also has broad applications for time-critical message delivery among electronic devices on physical infrastructures. However, the shared nature of wireless channels unavoidably exposes the messages in transit to jamming attacks, which broadcast radio interference to affect the network availability of electronic equipments. In time critical wireless communication system (e.g., messages in power substations have latency constraints ranging from 3 ms to 500 ms), the delivery of messages is expected to be followed by a sequence of actions on physical infrastructures [6], [7]. Over-due message delivery may lead to instability of system operations, and even cascading failures. For instance, in the smart grid, a binary result of fault detection on a power feeder can trigger subsequent operations of circuit breakers. If the message containing such a result is missed, or does not arrive on time, the actions on circuit breakers will be delayed, which can cause fault propagation along physical infrastructures and potential damages to power equipments. Under laid device-to-device (D2D) users communicate directly by utilizing the cellular spectrum but their decisions are not governed by any centralized controller [8]. Selfish D2D users that compete for access to the resources form a distributed system where the transmission performance depends on channel availability and quality. This information, however, is difficult to acquire. Moreover, the adverse effects of D2D users on cellular transmissions should be minimized A recipient of a message needs to be guaranteed that the message came from its specified source and a message should only be accepted if it was not modified during communication. This can help to prevent attacks where an adversary listens, modify and rebroadcasts messages. All communications need to be kept private so that eavesdroppers or adversary cannot intercept study and captures the content of messages. Eavesdropper receive all network packets before reaching base station and generate or reprograms nodes with fake information about routes. Packet loss over wireless network incurs a great challenge over the system stability as well as its control performance in WSN-based cyber-physical systems [9]-[11]. A sensor node communicates with a remote estimator through a wireless channel which may be jammed by an external attacker and hence protecting this communication channel from malicious attacks is an important yet challenging security issue in mobile networks.

The rest of the paper is structured as follows: In Section II we define the basis for game theory modeling. In Section III we present the related work regarding different cyber security issues in wireless systems. Section IV presents the results of our game model. Section V presents the conclusions of our work.

II. Game Theory Modelling

Cyber security risk management in wireless networks has been a challenging problem for both practitioners and the research community. Their proprietary nature along with the complexity of those systems renders traditional approaches rather insufficient and creating the need for the adoption of a holistic point of view. Tools like Viable System Model and Game Theory are employed to present a novel systemic approach towards cyber security management in this field, taking into account the complex inter-dependencies and providing cost-efficient defense solutions. Game Theory is a mathematical tool that is used in situations (games) where participants (players) have conflicting interests. Every player can adopt a method of action (strategy) and for every possible combination of adopted strategies there is a reward/utility that occurs for each of them [12]. Game theoretic implementations can "solve" a game by detecting the most effective strategy that each player should adopt in order to maximize their personal reward/utility (assumption of rationality of players). Although there are many kinds of games and many different concepts for defining a "solution" for a game, in this work we only construct two-player games where every player loses exactly as much as the other wins (zero-sum game). By solving the game we mean finding, before the game starts (static game), a strategy for each player such that none of them would be tempted to unilaterally deviate by because that would lead to a worse individual reward (the concept of Nash Equilibrium) [13], [14]. For the purposes of our research we have constructed a game where the defender aims at protecting a cyber component using cost efficient strategies while the attacker tries to find the attack scenario that causes maximum possible damage.

The aim is to consider the faithful communication channel in wireless networks from the game-theoretic viewpoint and therefore provide the optimal strategies for both attacker and defender to constitute Nash equilibrium. One fundamental challenge for security design in mobile networks is the absence of any preexisting infrastructure support. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot [15]-[17]. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks

typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Differing evidently from conventional communication system, where throughput is one of the most important performance metrics to indicate how much data can be delivered during a time period, wireless networking for cyber-physical systems aims at offering reliable and timely message delivery between physical devices [18]. Hence the objective is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures. All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

III. Related Work

Game theoretic framework could be designed to highlight issues of cooperation and competition among multiple radios and multiple channels Game theory not only provides game models for efficient self-enforcing distributed design, but also derives well-defined equilibrium criteria to study the optimality of game outcomes for various game scenarios. Game theory explicitly recognizes the interdependence across radios; it can be used as a synthesis tool to provide distributed algorithms for adaptive resource allocation [19]. And the concept of equilibrium in a game provides a useful analysis tool. We can also say that detecting the activities of Pus (primary users) might be wrong, and when it comes to a collision, SUs (secondary users) can distinguish the collision which is happened with PUs or SUs. To resolve contention among cognitive radios, we can use CSMA (Carrier Sense Multiple Access) to randomly allocate channel times among competing cognitive radios based on a reservation system. Hence we can introduce an approach towards the cyber security risk management in wireless networks, utilizing principles from the Viable System Model (VSM) and Game Theory (GT), two widely known methods for organizational management and strategic decision-making respectively.

We can also analyze several non-cooperative games for joint transmitter and receiver optimization, and aimed at maximizing utility functions strictly related to the signal-to-interference plus noise ratio (SINR). For such games we analytically prove the existence of Nash equilibrium. We propose a non-cooperative joint transceiver optimization and transmit power control game aimed at maximization of the energy efficiency of each active user [20]-[23]. Energy efficiency, measured in bit/Joule, represents the number of bits that are *successfully* delivered at the receiver for each energy unit taken from the battery and used for transmission. Unfortunately, for such a game the existence of an NE is shown only through numerical evidence, since we were not able to obtain an analytical proof.

The resource utility and network throughput are both the key challenges in wireless multi-hop network. By introducing the idea of cross-layer design and its cooperative mechanism, a multi constrained optimization scheme could be used [24]-[26]. The proposed scheme combines the energy threshold in the physical layer and the channel capacity in the link layer and integrates the advantage of tight coupling and loose coupling methods. The bargaining game theory is applied to analyze the bargaining behavior of nodes in the network. This optimization scheme can efficiently improve the fairness and utility of the resource in the network.

Another approach is to use Bio-inspired Trust and Reputation Model (BTRM-WSN). BTRM-WSN carries out the selection of the most trustworthy node through the most reputable path offering a certain service. It is based on a bio-inspired algorithm called Ant Colony System (ACS), where ants build paths in order to fulfill certain conditions graphically [27]-[30]. These ants leave some pheromone traces that help next ants to find and follow those routes. These pheromone values will help ants find the optimal route solutions since the optimal path will have the largest amount of pheromone value. When we apply this ACS algorithm onto trust and reputation system, we use "pheromone value" to represent the trustworthiness of sensors. In this BTRM-WSN, each sensor contains pheromone traces for its neighbors ($\tau \in [0,1]$), which determines probability for an ant to select a path as well as the senor the path leading to as a solution. In other word, τ can be considered as the trust that a sensor gives another.

Literature survey also motivates a newly deployed solution that uses the placement of multiple base stations to improve the probability of packets from the SNs (sensor nodes) reaching at least one base station in the network, thus ensuring high packet delivery success [31]. Assumptions given that in a WSN a base station is a desktop or laptop class device, by considering such base stations the idea of deploying multiple BSs is inexpensive.

Another technique called SPREAD (Secure Protocol for Reliable Data Delivery) divides multiple shares by using the secret sharing technique and then transmits data shares to the destination through one or more independent paths. Here alternative of using the single shortest path to route data from one node to the other is

dropped. The SPREAD technique was shown to be effective in improving security. It is more resistant to collusion attacks of up to a certain number of compromised nodes. As per concern security, slight or no redundancy should be added to the information transmitted. The amount of information redundancy required makes security and reliability seemingly contradicting objectives for schemes based on multipath routing.

Another scheme called REWARD is based on routing algorithm to detect team malicious attacks in wireless sensor networks [32], [33]. In this technique, a packet transmission by transmitting sensor node performs power control to more than one sensor node in the direction of the BS (base station). If an SN that is on the route does not forward a packet, then its next hop neighbor on the forwarding route will identify this event happening and report the SN as a black hole. This is implemented in literature where routing technique is suitable for network nodes that can tune their transmit power. REWARD forwards packets using geographic routing. This algorithm employs two types of broadcast messages to unify a scattered data base for detected black hole attacks, namely MISS and SAMBA. Identification of malicious node working in the ID space can be done with the help of MISS. Location of the detected malicious node attack is provided by another message SAMBA which is related to the physical space. In this scenario, if a malicious node performances on behalf of another node then SAMBA messages will decline its efficiency. Certainly, additional energy is drawn from the batteries due to security overheads in WSNs. REWARD allows striking the balance between security capability and lifetime performance. This scheme is very expensive for a network with n malicious nodes, for each original message, it requires *O(n)* extra messages.

IV. SYSTEM MODEL

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers, i.e., the interactive decision theory. At the beginning, game theory was widely used in economics, political science, as well as psychology. Today, has found a growing number of application including communication, control and network protocol design.

Due to the energy limitation, suppose that within a time horizon *T*, the sensor can send the data packet at most $M \leq T$ times to the remote estimator while the attacker can launch jamming attack at most $N \leq T$ times.

Denote $\theta_s \triangleq \{\gamma_1, \gamma_{2,}\ldots, \gamma_T\}$ as the sensor's data-sending strategy, where $\gamma_k = 1$ means the sensor sends data packet at time *k*, otherwise $\gamma_k = 0$. Consequently we have:

$$\sum_{k=1}^{k=T} \gamma_k \leq M .$$

Similarly we denote $\theta_A \triangleq \{\lambda_1, \lambda_{2,}\ldots, \lambda_T\}$ as the attacker's attack strategy, where $\lambda_k = 1$ means the attacker launch jamming attack at time *k*, otherwise $\lambda_k = 0$. Similarly we also have:

$$\sum_{k=1}^{k=T} \lambda_\kappa \leq N .$$

Finally the estimation will be perfectly if and only if $\gamma_k(1-\lambda_k) = 1$.

In our work, for the case with energy constraint for both sides, i.e., $M < T$ and $N < T$, which is much general situation in practice, the tools provided in existing literature cannot be used. Since both sides have many different strategies and have to take the opponent's strategy into consideration, we will investigate the problem from a game-theoretic point of view.

To utilize the mature tools from the game theory, we need some basic and necessary assumptions:

Assumption 4.1: Both the senor and the attacker are intelligent rational decision makers, pursuing the maximization of their utilities, i.e., their payoff function (objective function) (25) and (24), respectively.

Remark 4.2: This "rational maximizing behavior" is a basic assumption in game theory, while it does not necessarily mean that people always make "100% perfect decisions", due to that people may be limited by the amount of information they have.

Definition 4.3: The common knowledge *p* in a group of players *G* is that all the players in *G* know *p*, they all know that they know *p*, they all know that they all know that they know *p*, and so on and so forth.

Assumption 4.4: The decision maker at each side acts simultaneously or, at least, without knowing the actions of the other. But they know the objective function and the possible actions set of each other, which is common knowledge among them.

Definition 4.5: A game consists of a set of players, a set of strategies available to those players, and a specification of payoffs for each player on the condition of each combination of strategies.

Definition 4.6: A player's *strategy* refers to one of all the options he can choose in the game, which will determine all the actions to take at any stage of the game.

A *pure strategy* provides a complete definition of how a player will play a game.

A player's *strategy set* is the set of all the pure strategies available to that player.

A *mixed strategy* is an assignment of probability to each pure strategy in the strategy set, which allows the player to randomly select a pure strategy.

A *strategy profile* (strategy combination) is a set of strategies for each player which fully specifies all actions in a game.

Remark 3.7: We can regard the pure strategy as a degenerate case of the mixed strategy, where the particular pure strategy is selected with probability 1 and every other strategy with probability 0.

If in the game, each player has chosen a strategy and no player can benefit by changing his own strategy while the other players keep their unchanged, then the current strategy profile, i.e., the current set of strategy choices constitute a Nash equilibrium. We can express the definition in an analytical way.

Now here we denote pure strategies as $\theta_s^{pure}(1)$, $\theta_s^{pure}(2), \dots, \theta_s^{pure}(K)$.Though the number of the pure strategy is finite; there are infinitely many mixed strategies for each side. Thus the mixed strategy for the sensor can be written as:

$$\theta_s^{mixed}\left(\pi_1, \pi_2, \pi_3, \dots, \pi_K\right) = \{\theta_s^{pure}(K)\ with\ probability\ \pi_K\},\quad k = 1, 2, \dots, K,$$

Where

$$\sum_{k=1}^{k=K} \pi_K = 1\ ,\ \pi_K \in [0,1].$$

Note that different combinations of $\{\pi_K\}$ constitute different mixed strategies.

For the attacker, we have similar notations as:

$$\theta_A^{mixed}\left(\square_1, \square_2, \square_3, \dots, \square_K\right) = \{\theta_A^{pure}(K)\ with\ probability\ \square_K\},\quad k = 1, 2, \dots, L,$$

Where

$$\sum_{k=1}^{k=K} \square_K = 1\ ,\ \square_K \in [0,1].$$

The optimal solution so-called "pure strategy" is indeed a special form of our general mixed strategy and there exists at least one Nash equilibrium point in the game.

We provide an example to show how to obtain the optimal strategies for both sides. We consider a simple scenario where the time-horizon is 5 and both sides are limited to only one chance to send data or launch attack, i.e., T = 5, M = 1, N = 1. We investigate the average cost, namely, α = 1.

The attacker has five pure strategies: $\theta_A^{pure}(1)$= {1,0,0,0,0}, $\theta_A^{pure}(2)$ = {0,1,0,0,0}, $\theta_A^{pure}(3)$ = {0,0,1,0,0}, $\theta_A^{pure}(4)$ = {0,0,0,1,0}, $\theta_A^{pure}(5)$= {0,0,0,0,1}.

Similarly, for the sensor, we have $\theta_S^{pure}(1)$= {1,0,0,0,0}, $\theta_S^{pure}(2)$= {0,1,0,0,0}, $\theta_S^{pure}(3)$ = {0,0,1,0,0}, $\theta_S^{pure}(4)$ = {0,0,0,1,0}, $\theta_S^{pure}(5)$= {0,0,0,0,1}.

Thus, with the help of Lagrange multiplier we can say that the optimal strategy for the sensor will be $\{\frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}, \frac{1}{5}\}$, i.e., randomly choose pure strategies {1,0,0,0,0}, {0,1,0,0,0}, {0,0,1,0,0}, {0,0,0,1,0}, {0,0,0,0,1} with same probability 0.2. For the attacker we have similar conclusion.

According to the analysis model discussed above, we first investigate the performance of two players' i.e. the attacker and the defender. Here we have considered the case where the players have two channels of the same quality, hence they can achieve identical throughput.

Now another case could be where each player has two interfaces, i.e. two channels CH_{high} and CH_{low} . One channel is working with a high data rate and the other is working with a changing data rate. The player 1 chooses channel 1 with the probability $\boldsymbol{\gamma}$, and the player 2 chooses channel 2 with the probability θ. So the mixed strategy Nash Equilibrium using Lagrange's method of partial derivatives is p* = {($\boldsymbol{\gamma}$, 1- $\boldsymbol{\gamma}$), (θ, 1- θ)}, which can achieve the maximum utility and the fairness of each player simultaneously. Here we can propose a mixed strategy channel selection algorithm to maximize the utility of each player. According to this algorithm we first calculate the probability of choosing CH_{high} and CH_{low} by using the Lagrange's method of partial derivatives. Now if probability of choosing CH_{high} is greater than 1, then choose CH_{high} else generate a random number *RN* uniformly distributed from 0 to 1 and if probability of choosing CH_{high} is greater than random number *RN*, then choose CH_{high} else choose CH_{low}.

Here we can consider four situations for these asymmetrical channels: 1) mixed strategy channel selection algorithm (MS); 2) random channel selection (RS); 3) both players share the high rate channel (SH); 4) both players share the low rate channel (SL). Analyzing the throughput of four different strategies, we can say that mixed strategy can get the best performance in any situation. When the discrepancy of two channels is significant, MS can choose CH_{high} with higher probability, whereas RS chooses both channels randomly leading to a degradation of network performance. With the discrepancy of two channels decreasing, the probability of choosing CH_{high} in MS approaches to 0.5, and the throughput of RS is close to the one of MS. The throughput of SH is worse than MS, because it cannot make full use of other orthogonal channel to avoid the collision. The performance of SL is worst due to the lower rate and competition.

With the number of players increasing, MS always achieves the better performance than other schemes. SH

gets the higher throughput than RS, when the number of player is less. That is because the advantage of high rate channel is enough to accommodate these players. But when there are too many players, the competition on the higher rate channel is serious, so RS is better than SH. SL still gets the worst performance.

V. CONCLUSION

The motivation lies in the faithful transmission of confidential data over wireless channel and hence to provide a secure, reliable communication network. There are energy constraints for both the defender and the attacker, so the interactive decision making process between the sensor node and the attacker is investigated. A game-theoretical framework is formulated to prove that the optimal strategies for both sides constitute Nash equilibrium and hence improve the network throughput greatly. Also, the asymmetric multi-channel selection problem in a mobile network is comprehended using game theory and we analyzed that mixed strategy channel selection algorithm is a promising approach to achieve higher throughput in any situation. A sensor node communicates through a wireless channel which may be jammed by an external attacker, hence protecting this communication channel from malicious attacks in order to provide a reputable communication path is a challenging security issue in wireless networks.

REFERENCES

[1] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems.* ACM, 2012, pp. 47–54.

[2] Heena Rathore, Abhay Samant, "A system for building immunity in social networks", *in proc. Fourth World Congress on Nature and Biologically Inspired Computing* (NaBIC), no.4, pp. 20-24, 2012.

[3] Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher, "Challenges for Security in Wireless sensor Networks (WSNs)," *World Academy of Science, Engineering and Technology* 56 2011.

[4] Murad A. Rassam, M.A. Maarof and Anazida Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks," *American Journal of Applied Sciences*, vol. 9, no. 2, pp. 69-83, 2012.

[5] T. Spyridopoulos, T. Tryfonas, and J. May, "Incident analysis and digital forensics in SCADA and industrial control systems," *in System Safety Conference incorporating the Cyber Security Conference* 2013, 8th IET International, 2013, pp. 1-6.

[6] L. Shi, K. Johansson, and L. Qiu, "Time and event-based sensor scheduling for networks with limited communication resources," *in World Congress of the International Federation of Automatic Control (IFAC)*, 2011.

[7] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[8] Setareh Maghsudi and Sławomir Sta´nczak, Senior Member, IEEE, " Channel Selection for Network-assisted D2D Communication via No-Regret Bandit Learning with Calibrated Forecasting," *IEEE Transactions on Wireless Communications*, 10.1109/TWC.2014.2365803, 2013.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack policy against remote state estimation," *in 12th European Control Conference, Zurich, Switzerland*, July 2013 (submitted).

[10] M. Zuba, Z. Shi, Z. Peng, and J. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*. ACM, 2011, p. 12.

[11] L. Shi, M. Epstein, and R. Murray, "Kalman filtering over a packet dropping network: A probabilistic perspective," *Automatic Control, IEEE Transactions on*, vol. 55, no. 3, pp. 594 –604, march 2010.

[12] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," *in System Sciences (HICSS), 2010 43rd Hawaii International Conference on IEEE*, 2010, pp. 1–10.

[13] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE*,2013.

[14] W. Zhong, G. Chen, S. Jin, and K.-K. Wong, "Relay selection and discrete power control for cognitive relay networks via potential game," *IEEE Transactions on Signal Processing*, vol. 62, no. 20, pp. 5411–5424, Oct 2014.

[15] D. Kalathil, N. Nayyar, and R. Jain, "Decentralized learning for multiplayer multiarmed bandits," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2331–2345, April 2014.

[16] C. Xu, L. Song, Z. Han, Q. Zhao, X. Wang, X. Cheng, and B. Jiao, "Efficiency resource allocation for device-to-device underlay communication systems: A reverse iterative combinatorial auction based approach," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 348–358, Sept 2013.

[17] M. Tambe and B. An, "Game Theory for Security: A Real-World Challenge Problem for Multiagent Systems and Beyond," *Association for the Advancement of Artificial Intelligence*, 2011.

[18] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," *in Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011.

[19] Y. Xu, Q. Wu, J. Wang, L. Shen, and A. Anpalagan, "Opportunistic spectrum access using partially overlapping channels: Graphical game and uncoupled learning," *IEEE Transactions on*

Communications, vol. 61, no. 9, pp. 3906–3918, Sep 2013.

[20] Yang Dejun, Fang Xi, Xue Guoliang. "Channel Allocation in Noncooperative Multi-Radio Multi-Channel Wireless Networks", INFOCOM 2012, pp.882-890, 2012.

[21] Wen Jingrong, Wu Muqing, Tang Xiong. "Multi-Radio Multi-Channel Allocation in Competitive Wireless Ad hoc Networks*", The 75th IEEE Vehicular Technology Conference, VTC* 2012-spring, pp.

[22] M. Tanaka, D. Umehara, M. Morikura, N. Otsuki, and T. Sugiyama, "New throughput analysis of long-distance IEEE 802.11 wireless communication system for smart grid," in *Proc.IEEE SmartGridComm*, 2011.

[23] X. Lu, Z. Lu, W. Wang, and J. Ma, "On network performance evaluation toward the smart grid: A case study of DNP3 over TCP/IP," in *Proc. IEEE GLOBECOM, Houston*, TX, USA, Dec. 2011.

[24] John Felix Charles Joseph, Bu-Sung Lee, Amitabha Das, Boon-Chong Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 233-245, 2011.

[25] A. Cassola, T. Jin, G. Noubir, and B. Thapa, "Efficient spread spectrum communication without preshared secrets," *IEEE Trans. Mobile Comput.*, vol. 12, no. 8, pp. 1669–1680, Aug. 2013.

[26] E. Casini, A. van der Zanden, R. Goode, and R. Berto-Monleon, "IP QoS with military precedence level for the NATO information infrastructure," *in Proc. IEEE MILCOM, Baltimore*, MD, USA, Nov. 2011.

[27] Falko Dressler , Ozgur B. Akan, "A survey on bio-inspired networking", *Elsevier Computer Networks Journal*, vol. 54, no. 6, pp. 881900, 2010.

[28] Heena Rathore, Sushmita Jha, "Bio-Inspired Machine Learning Based Wireless Sensor Network Security", *Fifth world Congress on Nature and Biologically Tnspired Computing*, 2013.

[29] Yenumula B. Reddy , "Trust-Based Approach in Wireless Sensor networks using an Agent to each Cluster," *International Journal of Security, Privacy and Trust Management*, voU, no.l, pp. 19-36,2012.

[30] Gomez Marmol, Felix, and Gregorio Martnez Perez. "Providing trust in wireless sensor networks using a bio-inspired technique." *Telecommunication systems*, vol. 46, no. 2, pp. 163-180,2011.

[31] Satyajayant Misra, Kabi Bhattarai and Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks*", publication in the IEEE ICC* 2011 proceedings.

[32] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", *Journal of computing*, vol. 3, no. 1, pp. 41-48, 2011.

[33] Hichem Sedjelmaci and Mohamed Feham, "Novel Hybrid Intrusion Detection System for clustered wireless sensor network", *International Journal of Network Security and Its Applications*, vol.3, no.4, pp. 1-14, 2011.

