51st IEEE Conference on Decision and Control
December 10-13, 2012. Maui, Hawaii, USA

Game-Theoretic Analysis of Node Capture and Cloning Attack with Multiple Attackers in Wireless Sensor Networks

Quanyan Zhu, Linda Bushnell and Tamer Başar

Abstract— **Wireless sensor networks are subject to attacks such as node capture and cloning, where an attacker physically captures sensor nodes, replicates the nodes, which are deployed into the network, and proceeds to take over the network. In this paper, we develop models for such an attack when there are multiple attackers in a network, and formulate multi-player games to model the noncooperative strategic behavior between the attackers and the network. We consider two cases: a static case where the attackers' node capture rates are time-invariant and the network's clone detection/revocation rate is a linear function of the state, and a dynamic case where the rates are general functions of time. We characterize Nash equilibrium solutions for both cases and derive equilibrium strategies for the players. In the static case, we study both the single-attacker and the multi-attacker games within an optimization framework, provide conditions for the existence of Nash equilibria and characterize them in closed forms. In the dynamic case, we study the underlying multi-person differential game under an open-loop information structure and provide a set of conditions to characterize the open-loop Nash equilibrium. We show the equivalence of the Nash equilibrium for the multi-person game to the saddle-point equilibrium between the network and the attackers as a team. We illustrate our results with numerical examples.**

I. Introduction

Wireless sensor networks are networks of low-power, resource-limited embedded sensors, interacting and communicating to carry out a desired task. They are not only essential for military and large scale industrial systems, but are important in our every day lives in areas such as health monitoring [1] and environmental sampling [2]. These systems are usually unattended and are therefore vulnerable to many types of attacks. In this paper, we study the node capture and cloning attack [3], where an attacker captures a sensor node, extracts data, and uses the data to strategically deploy functional copies, or clones, into the network. The attacker uses the compromised sensors and clones to inflict damage on the network's operation.

As pointed out in [4], existing adversary models in the network security literature, including Byzantine failure [5] and Dolev-Yao [6] threat models are not adequate to model node capture and cloning attacks, which use only captured nodes and clones to damage a sensor network. Currently, there does not exist any other adversarial model for such attacks.

In this paper, we present a systematic approach to model and analyze the behavior of a wireless sensor network under a node capture and cloning attack. Specifically, we focus on the strategic interaction between the network and the attackers. We model and analyze the general case when there are multiple attackers using static and dynamic game theory. Our contributions can be summarized as follows.

- We develop dynamical models for the node capture and cloning attack when there are multiple attackers under general controller inputs from the attackers and the network.
- We study the static case when the attackers' controllers are time-invariant and the network's controller is a linear function of the state. We analyze both the single-attacker and the multi-attacker games within an optimization framework and characterize Nash equilibria in closed forms.
- We study the dynamic case when the rates are general functions of time. We analyze the multi-person differential game under an open-loop information structure and provide a set of conditions to characterize the open-loop Nash equilibrium. For a single attacker, we show the equivalence of the two-person nonzero-sum game to a zero-sum game. For the case of multiple attackers, we show the equivalence of the Nash equilibrium for the multi-person game to the saddle-point equilibrium between the network and the attackers as a team.
- We demonstrate our results through a simulation study with numerical examples, and compare the case of a single attacker to the case of multiple attackers.

The paper is organized as follows. In Section II, we discuss related work in this area. In Section III, we develop general models of the node capture and cloning attack for multiple attackers, and give preliminaries on the cost functions used to solve the problems. In Section IV, we present the static case. In Section V, we study the dynamic counterpart. In Section VI, we illustrate the equilibrium solutions of the games using numerical examples. Section VII concludes the paper.

II. Related Work

The node capture and cloning attack, which has been shown to be effective in subverting network processes such as data aggregation tasks, was first introduced in the security of wireless networks literature in [3]. Many detection algorithms for node capture and cloning attacks use distributed protocols that rely on collisions of messages containing

The research was supported in part by the AFOSR MURI Grant FA9550-10-1-0573, and also by an NSA Grant through the Information Trust Institute at the University of Illinois.

Q. Zhu and T. Başar are with the Coordinated Science Laboratory and Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA. Email: {zhu31, basar1}@illinois.edu

L. Bushnell is with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA. Email: lb2@uw.edu

978-1-4673-2066-5/12/$31.00 ©2012 IEEE

unique IDs and locations [4], [8], [9]. These methods assume that each captured node is cloned at least once.

Game theory has been widely considered as an appropriate tool to model behaviors of attackers, [10], [11]. There have been a few papers that have employed static and dynamic game theory tools to study security problems in different scenarios. In [12], we have used a zero-sum game-theoretic framework to study jamming attacks in delay-tolerant networks. The source nodes in the network strategically choose transmission probabilities to maximize the probability of successful delivery of contents while an adversary aims to cause a maximum number of collisions. In [13], we have introduced a stochastic game to model the interactions between a jammer and a secondary user in a cognitive radio system. The primary users in the network control the states and state transitions while the jammer acts against the secondary users under all channel states. In [14], we have formulated a noncooperative game to analyze the complex interactions between wireless users and a malicious node in the context of relay station-enabled wireless networks.

Control theory has been used recently to model attacks on wireless sensor networks. In [15], an attacker compromises a subset of sensors in a wireless sensor network and injects false data into the network to alter a state estimation task. The effect of the false data is analyzed as a constrained control problem. In [16], an attacker with limited knowledge of the network and unlimited resources injects false data into a Supervisory Control and Data Acquisition (SCADA) system operating on power grids. The state estimates are analyzed under a cyber security attack. These two papers model the impact of the false data injection attack as additive noise. In [17], we have investigated the coupling between physical layer control system design and the cyber level intrusion attacks. A novel framework is built upon game theory and control theory to analyze and design robust and resilient controllers for cyber-physical systems. In [7], we have introduced a linear dynamical model for the node capture and cloning attack with a single attacker when the state is the number of captured nodes in the network, the attacker's capture rate is time-invariant, and the network's detection rate is a linear function of the state.

III. Model and Preliminaries

In this section, we formulate a game-theoretic framework to model the strategic interactions between the network and multiple attackers. We first introduce a linear system model to describe the dynamical interactions between the node capturing, cloning and revocation processes. Then we describe the cost functions using cryptographic parameters.

A. System Model

As shown in Figure 1, the network consists of a large number of wireless sensors distributed over some given area. The attacker mounting a node capture and cloning attack in one neighborhood will capture a node and create at least one functional copy of the node, which is placed in a different neighborhood.

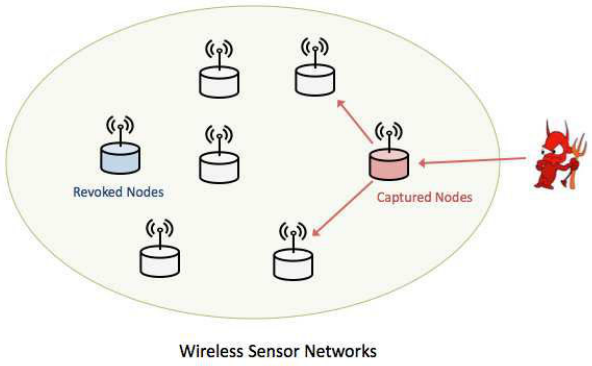


Fig. 1. Wireless sensor networks: attackers capture nodes, replicate them, and then use the captured nodes and clones to inflict damage on network operations. The network detects the compromised nodes, revokes them, and replaces them with new nodes.

The linear dynamical model from [7] can be generalized to provide a more flexible model that includes multiple attackers and time-varying capture and revocation rates. Let λ be the capture rate of an attacker and μ be the revocation rate of the network. Since the network consists of a large number of wireless sensors, we can use a continuum state $x(t) \in [0,1]$ to denote the fraction of captured nodes among all sensors. The state evolves according to the following dynamics:

$$\dot{x}(t) = \lambda[1-x(t)] - \mu,\ x(0) = x_0, \tag{1}$$

where $x_0 \in [0,1]$ is the initial condition of the system. Note that x is a state variable that has been normalized by the size of the total node population. The control variable for the attacker, λ, can be either a constant or a time varying function depending on the states. Likewise, the controller μ for the network can also take different forms. In this paper, we study two scenarios, one is the static case and the other one is the dynamic case. In the static case, we let λ be a time-invariant parameter and take μ as a linear function of the state variable $x(t)$, i.e., $\mu = ux$, for some $u \in \mathbb{R}$. In the dynamic case, we set μ and λ as control variables as functions of information structures $\eta_{\mathscr{N}}(\cdot)$, $\eta_{\mathscr{A}}(\cdot)$ for the network and the attacker, respectively. $\eta_{\mathscr{N}}(\cdot)$, $\eta_{\mathscr{A}}(\cdot)$ are set valued functions defined as

$$\eta_e(t) = \{x(s),\ \ 0 \le s \le \varepsilon_t^e\},\ 0 \le \varepsilon_t^e \le t, e \in \{\mathscr{N},\mathscr{A}\},$$

where ε_t^e is nondecreasing in t, and $\eta_e(t), e \in \{\mathscr{N},\mathscr{A}\}$, determines the state information gained and recalled by each player at time $t \in [0,T]$. For example, for open-loop (OL) information structure, $\eta_e^{\mathrm{OL}}(t) = \{x_0\}, e \in \{\mathscr{N},\mathscr{A}\}$, and, for closed-loop perfect state (CLPS) information structure, $\eta_e^{\mathrm{CLPS}}(t) = \{x(s), 0 \le s \le t\}, t \in [0,T], e \in \{\mathscr{N},\mathscr{A}\}$. The interested readers can refer to [19] and [20] for more discussion on various information structures.

The dynamics (1) can be generalized to study multiple attackers. We consider the case where the attackers are

cooperating and derive the dyanmical equation as follows:

$$\dot{x}(t) = \left(\sum_{i=1}^{p} \lambda_i\right)[1-x(t)] - \mu,\ x(0) = x_0, \tag{2}$$

where now the network is subject to p attackers, $\mathscr{A}_i, i = 1,2,\cdots,p$, each using its capture rate λ_i to inflict damage on the network. Multiple attackers will be analyzed for both the static and dynamic game scenarios as described above.

B. Cost Functions

The goal of each attacker is to inflict damage on the network, while the network aims to protect itself and recover from the damages. The goals of the players can be captured by cost functions $J_{\mathscr{A}_i}, i = 1,2,\cdots,p$, for the attackers and $J_{\mathscr{N}}$ for the network. The cost functions are dependent on pre-specified cryptographic parameters and dictate the optimal strategies of the players.

We assume that attackers $\mathscr{A}_i, i = 1,2,\cdots,p$, each incur two types of costs when carrying out a node capture and cloning attack: the cost of capturing a node, C_{i1}, and the cost of disrupting the remaining valid nodes in the network, C_{i2}. Similarly, the network incurs the cost of having compromised nodes within the network, C_{01}, and the cost of detecting, revoking, and replacing compromised nodes, C_{02}. We choose to analyze this problem with the following costs for the attackers, for $i = 1,\cdots,p$, and the network:

$$C_{01} := \lim_{T\to\infty} \frac{1}{T}\int_0^T r_0 x(t)^2\,dt, \tag{3}$$

$$C_{02} := \lim_{T\to\infty} \frac{1}{T}\int_0^T q_0 \mu^2\,dt, \tag{4}$$

$$C_{i1} := \lim_{T\to\infty} \frac{1}{T}\int_0^\infty q_i \lambda_i^2 z(t)^2\,dt, \tag{5}$$

$$C_{i2} := \lim_{T\to\infty} \frac{1}{T}\int_0^\infty r_i z(t)^2\,dt, \tag{6}$$

where $z(t)$ is the fraction of the remaining valid nodes, $z(t) := 1-x(t)$, and the dynamics can be rewritten from (2) into:

$$\dot{z}(t) = -\left(\sum_{i=1}^{p} \lambda_i\right) z(t) + \mu,\ z(0) = z_0 := 1 - x_0. \tag{7}$$

The cryptographic parameters r_0, q_0 for the network and r_i, q_i for the attackers, $i = 1,2,\cdots,p$, are given unit cost values based on the system under study. The above cost functions are quadratic, specifically containing a square term of the state or rate. Future work will generalize these to functions including linear terms.

IV. Static Case

In this section, we analyze the node capture and cloning attack when the capture rates are time-invariant and the revocation rate is a linear function of the state. We first develop models and the game structure, then derive solutions for both a single attacker and multiple attackers.

Recalling the dynamics (2), we let the network controller take the form $\mu = ux$ and let $u, \lambda_i \in [0,1], i = 1,2,\cdots,p$. Attacker $\mathscr{A}_i$ aims to increase the number of captured nodes in the network with minimal control, which can be modeled by the following cost functions, using the costs from (5), (6):

$$J_{\mathscr{A}_i}(\lambda_i, \lambda_{-i}, u) := \lim_{T\to\infty} \frac{1}{T}\int_0^T [r_i z(t)^2 + q_i \lambda_i^2 z(t)^2]\,dt, \tag{8}$$

where $\lambda_{-i} := \{\lambda_j, j \neq i, j = 1,2,\cdots,p\}$ is the set of actions of attackers other than i, and $z(t)$ from (7) now has the form:

$$\dot{z}(t) = -\left(\sum_{i=1}^{p} \lambda_i\right) z(t) + u(1-z(t)),\ z(0) = z_0. \tag{9}$$

The network's goal is to increase the number of valid nodes while minimizing the revocation rate, which can be modeled by the following cost function, using the costs from (3), (4):

$$J_{\mathscr{N}}(\lambda_i, \lambda_{-i}, u) := \lim_{T\to\infty} \frac{1}{T}\int_0^T [r_0 x(t)^2 + q_0 u^2 x(t)^2]\,dt, \tag{10}$$

where $x(t)$ from (2) now has the form:

$$\dot{x}(t) = \left(\sum_{i=1}^{p} \lambda_i\right)[1-x(t)] - ux(t),\ x(0) = x_0. \tag{11}$$

In this section, we solve for Nash equilibrium (NE) solutions for the differential games described by (8), (9), (10), and (11). This structure leads to showing convexity of the optimization problems and using the concept of best responses [19] for deriving NE for the optimal actions of the players.

Definition 1: Consider the static game described by the dynamics (11) and the cost functions $J_{\mathscr{A}_i}(\lambda_i, \lambda_{-i}, u)$ and $J_{\mathscr{N}}(\lambda_i, \lambda_{-i}, u)$ as defined above. The set of strategies $\{u^*, \lambda_i^*, i = 1,2,\cdots,p\}$, constitutes a Nash equilibrium solution if, and only if, the following inequalities are satisfied for all u and $\lambda_i \in [0,1], i = 1,2,\cdots,p$:

$$\begin{aligned} J_{\mathscr{A}_i}(\lambda_i^*, \lambda_{-i}^*, u^*) &\leq J_{\mathscr{A}_i}(\lambda_i, \lambda_{-i}^*, u^*), \\ J_{\mathscr{N}}(\lambda_i^*, \lambda_{-i}^*, u^*) &\leq J_{\mathscr{N}}(\lambda_i^*, \lambda_{-i}^*, u). \end{aligned}$$

A. Static Case: Single Attacker

Equation (11) with one attacker reduces to the form:

$$\dot{x}(t) = \lambda_1[1-x(t)] - ux(t),\ x(0) = x_0. \tag{12}$$

By solving this ODE, we can derive the fraction of captured nodes present in the network at time t as:

$$x(t) = e^{-(\lambda_1+u)t}x_0 + \frac{\lambda_1}{\lambda_1+u}[1 - e^{-(\lambda_1+u)t}]. \tag{13}$$

The cost function for the network is as in (10). The attacker's cost function is given in (8) with $i = 1$.

The optimization problem for the attacker is:

$$\begin{aligned} &\min_{\lambda_1} \lim_{T\to\infty} \frac{1}{T}\int_0^T [r_1 z(t)^2 + q_1 \lambda_1^2 z(t)^2]\,dt \\ &\text{s.t. } \dot{z}(t) = -\lambda_1 z(t) + u[1-z(t)]\ ,\ \lambda_1 \in [0,1] \end{aligned} \tag{14}$$

The optimization problem for the network is:

$$\begin{aligned} &\min_{u} \lim_{T\to\infty} \frac{1}{T}\int_0^T [r_0 x(t)^2 + q_0 u^2 x(t)^2]\,dt \\ &\text{s.t. } \dot{x}(t) = \lambda_1[1-x(t)] - ux(t)\ ,\ u \in [0,1] \end{aligned} \tag{15}$$

If we assume $x_0 = 0$, substituting (13) into (15) simplifies the network's optimization problem to:

$$\min_u \frac{\lambda_1^2}{(\lambda_1+u)^2}[r_0 + q_0 u^2] \quad \text{s.t. } u \in [0,1] \tag{16}$$

Proposition 1: Let $k_0 = r_0/q_0$. The best response function $B_0 : [0,1] \to [0,1]$ of the network to the attacker's action $\lambda_1 \in [0,1]$ is given by

$$u = B_0(\lambda_1) := \begin{cases} k_0/\lambda_1, & \lambda_1 > k_0, k_0 < 1 \\ 1, & \lambda_1 \le k_0, k_0 < 1 \text{ or } k_0 \ge 1 \end{cases}$$

Proof: Define the objective function as: $F(u) := \lambda_1^2[r_0 + q_0u^2]/(\lambda_1+u)^2$. We compute its first derivative:

$$F'(u) = \frac{2\lambda_1^2}{(\lambda_1+u)^3}[q_0 u\lambda_1 - r_0].$$

$F'(u)$ is negative at $u = 0$ and, depending on the value of λ_1, it either remains negative for the entire range of values of u or changes sign from negative to positive (and only once), and this happens at $u = k_0/\lambda_1$ if $\lambda > k_0$. Hence, for $k_0 < 1$, the best response function is $B_0 = 1$ when $F'(u)$ is negative for $u \in [0,1]$, i.e., $\lambda_1 \le k_0$; the best response is given by $B_0 = k_0/\lambda_1$ when $\lambda_1 \ge k_0$.. ∎

Similarly, we can obtain the best response function B_1 for the single attacker.

Proposition 2: Let $k_1 = r_1/q_1$. The best response function $B_1 : [0,1] \to [0,1]$ is given by

$$\lambda_1 = B_1(u) := \begin{cases} k_1/u, & u > k_1, k_1 < 1 \\ 1, & u \le k_1, k_1 < 1 \text{ or } k_1 \ge 1 \end{cases}$$

Proof: Note that the utility function for the attacker has the same form as the network, and the result directly follows from the proof of Proposition 1. ∎

Theorem 1: The Nash equilibrium of the two-person static game between one attacker and the network is unique for the cases (i) $k_0 < k_1 \le 1$ (or $k_0 < 1$, $k_1 > 1$) and (ii) $k_1 < k_0 \le 1$ (or $k_1 < 1, k_0 > 1$). The solution (u^*, λ_1^*) is given in these cases respectively by (i) $u^* = k_0, \lambda_1^* = 1$, (ii) $u^* = 1, \lambda_1 = k_1$. If $k_0 = k_1 =: k < 1$, then there is a continuum of NE, i.e., any (u^*, λ_1^*) on the curve $u^*\lambda_1^* = k$, with $k \le u^*, \lambda_1^* \le 1$, is a NE; and if $k_0 \ge 1$ and $k_1 \ge 1$, then NE is again unique and is given by $u^* = \lambda_1^* = 1$.

Proof: NE is the intersection point of two best-response functions B_0 and B_1. The result follows from finding the intersection points in different regions. ∎

As an example, in Fig. 2, we depict the best response functions of the two-person game and its NE. We show the NE solution described by Theorem 1 in three different regions of the parameter space.

B. Static Case: Multiple Attackers

For the case with p attackers, we use the linear model from (11). The cost function for the network is the same as in (10). The cost functions for the attackers follow from (8) with λ_i, q_i, r_i as parameters for $i = 1, \cdots, p$.

The optimization problem for the network is (with initial condition $x_0 = 0$):

$$\min_u \frac{\left(\sum_{i=1}^p \lambda_i\right)^2}{\left(\sum_{i=1}^p \lambda_i + u\right)^2}[r_0 + q_0 u^2] \quad \text{s.t. } u \in [0,1] \tag{17}$$

The p optimization problems for the attackers (with $z_0 = 1$) are, for $i = 1, \cdots, p$:

$$\min_{\lambda_i} \frac{u^2}{(\lambda_i+u)^2}[r_i + q_i\lambda_i^2] \quad \text{s.t. } \lambda_i \in [0,1] \tag{18}$$

In the multiple attacker case, due to the symmetry and resemblance of the problem to (16), the best-response function $u = \bar{B}_0(\lambda_1, \lambda_2, \cdots, \lambda_p) : [0,1]^p \to [0,1]$ for the network is given by

$$u := \begin{cases} \frac{k_0}{\sum_{i=1}^p \lambda_i}, & \sum_{i=1}^p \lambda_i > k_0, k_0 < 1 \\ 1, & \sum_{i=1}^p \lambda_i \le k_0, k_0 < 1 \text{ or } k_0 \ge 1 \end{cases} \tag{19}$$

With $k_i = r_i/q_i$, the best-response function $B_i : [0,1] \to [0,1]$ for attacker $i = 1, \cdots, p$ is given by

$$\lambda_i = B_i(u) := \begin{cases} k_i/u, & u > k_i, k_i < 1 \\ 1, & u \le k_i, k_i < 1 \text{ or } k_i \ge 1 \end{cases} \tag{20}$$

From (19) and (20), we can see that the best-response function of attacker i is dependent on the network action u only. Hence we can define the aggregate attack response $B_A(u) = \sum_{i=1}^n B_i(u)$. Without loss of generality, we order the indices of attackers according to their value k_i, i.e., $k_1 \le k_2 \le \cdots \le k_{p_n} \le 1 \le k_{p_n+1} \le k_{p_n+2} \le \cdots \le k_p$. The best response B_A can thus be obtained as follows.

$$B_A(u) := \begin{cases} p, & u < k_1 \\ (p - i - I(k_i)) + \frac{1}{u}\sum_{j=i}^{\mathscr{I}(k_i)} k_j, & cond.2 \\ (p - p_n) + \frac{1}{u}\sum_{j=1}^{p_n} k_j, & k_{p_n} \le u < 1 \end{cases} \tag{21}$$

where $\mathscr{I}(k_i) = \max\{h : k_h = k_i, h = 1,2,\cdots,p\}$, $I(k_i) = \mathscr{I}(k_i) - i$, and *cond. 2* is $k_i \le u < k_{i+1}, i = 1, \cdots, p_n - 1, k_i \ne k_{i+1}$.

Theorem 2: There exists a Nash equilibrium for the $(p+1)$-person static game.

Proof: Let $f_B(u) := \bar{B}_0(B_A(u))$. A NE satisfies the fixed point equation $u = f_B(u), u \in [0,1]$. Since the best response functions $\bar{B}_0, B_A$ are continuous over the compact sets $[0,p]$ and $[0,1]$, respectively, the result follows from invoking Brouwer's fixed point theorem [18]. ∎

In the following, we discuss several special cases and show that the multi-attacker game admits either a unique equilibrium or multiple equilibria, depending on the parameters.

Corollary 1: Suppose that $k_0 = k_1 = \cdots = k_p := k < 1$. Then, the $(p+1)$-person static game admits a unique NE solution $u^* = k/p, \lambda_i^* = 1, i = 1, 2, \cdots, p$.

Proof: The proof follows from finding the best response curves $\bar{B}_0$ and B_A, and they have only one intersection point, which yields the NE. ∎

Corollary 2: Suppose that $k_1 = \cdots = k_p := k < 1$ and $k_0 = pk$. Then, the $(p+1)$-person static game has a set of NE solutions given by $\{(u^*, \lambda_1^*, \lambda_2^*, \cdots, \lambda_p^*) : \lambda_1^* = \lambda_2^* = \cdots = \lambda_p^* := \lambda^*, u^*\lambda^* = k, \lambda^* \in [0,1], u^* \in [0,1]\}$

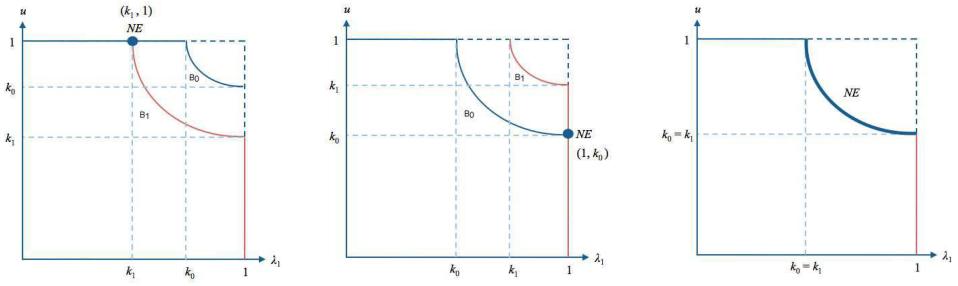


Fig. 2. The NE solution for a static game between one attacker with $k_1 = r_1/q_1$ and the network with $k_0 = r_0/q_0$. The blue curve is the best response function B_0 of the network to the attacker, and the red curve is the best response function B_1 of the attacker to the network. The NE is the intersection point of two best response curves. We illustrate three cases of NE solutions: (a) $k_1 < k_0 < 1$: NE solution is obtained at $\lambda_1^* = k_1, u^* = 1$; (b) $k_0 < k_1 < 1$: NE solution is $\lambda_1^* = 1, u^* = k_0$; (c) $k_0 = k_1 < 1$; NE solutions are points on the highlighted curve, i.e., $u^*\lambda_1^* = k_0 = k_1$.

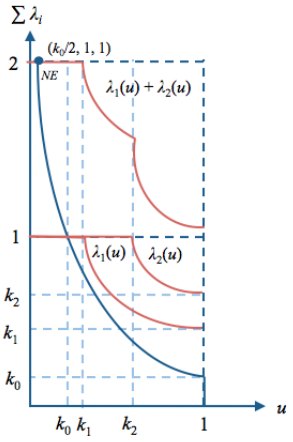


Fig. 3. The NE solution for a static game with two attackers. The BR of the two attackers are depicted by $\lambda_1(u)$ and $\lambda_2(u)$, respectively. The BR of the network is depicted by the blue curve. With $k_0 < k_1 < k_2 < 1$, the NE solution is achieved at $u = k_0/2, \lambda_1 = 1, \lambda_2 = 1$.

Proof: It is easy to show that, for any NE, it must satisfy $\sum_{i=1}^{p} \lambda_i u = kp$. Due to symmetry, all λ_i at equilibrium must be the same, i.e., $\lambda_i := \lambda$ for all $i = 1, \cdots, p$, $u\lambda = k$. The result then follows from using the condition $\lambda = B_i(u)$. ■

In Fig. 3, we use an example to illustrate the result in Theorem 2. The best response functions of the network and the attackers are illustrated. The equilibrium solution depends on the parameters in the best response functions.

V. Dynamic Case

In this section, we analyze the dynamic case of the node capture and cloning attack on a wireless sensor network when there are multiple attackers. We first develop the single attacker case for comparison.

The general form of the dynamics for the fraction of compromised nodes has been described in (2) and (7) in Section III. Attacker $\mathscr{A}_i$ aims to increase the number of captured nodes with minimum control, which can be modeled by the following cost functions:

$$J_{\mathscr{A}_i}(\lambda_i, \lambda_{-i}, \mu) := \int_0^T r_i z^2 + q_i \lambda_i^2 dt, \tag{22}$$

for $i = 1, 2, \cdots, p$. Note that the dependence of cost function $J_{\mathscr{A}_i}$ on the actions of the other players comes from the state dynamics (7).

On the other hand, the network's goal is to increase the number of healthy nodes while minimizing the revocation rate, i.e., the player minimizes the following cost function:

$$J_{\mathscr{N}}(\lambda_i, \lambda_{-i}, \mu) := \int_0^T (-r_0 z^2 + q_0 \mu^2) dt. \tag{23}$$

Here we are not requiring λ and μ to be in [0,1]. We should make that explicit. In this section, we look for open-loop NE solutions for the differential game described by (7), (22) and (23). A strategy is said to be open loop (OL) if it does not depend on the state of the system, i.e, $\lambda_i = \bar{\lambda}_i(t, z_0) \in \Lambda_i$ and $\mu = \bar{\mu}(t, z_0) \in \Gamma$, where $\bar{\lambda}_i$ and $\bar{\mu}$ are continuous in t, and Λ_i and Γ are strategy spaces of attacker $\mathscr{A}_i$ and the network, respectively, containing permissible open loop strategies.

Definition 2: Let $\bar{J}_{\mathscr{A}_i} := J_{\mathscr{A}_i}(\bar{\lambda}_i, \bar{\lambda}_{-i}, \bar{\mu})$ and $\bar{J}_{\mathscr{N}} := J_{\mathscr{N}}(\bar{\lambda}_i, \bar{\lambda}_{-i}, \bar{\mu})$. The set of strategies $\{\bar{\mu}^*, \bar{\lambda}_i^*, i = 1, 2, \cdots, p\}, \bar{\lambda}_i^* \in \Lambda_i, \bar{\mu}^* \in \Gamma$, constitutes an open-loop (OL) NE solution if, and only if, the following inequalities are satisfied for all $\bar{\mu} \in \Gamma$ and $\bar{\lambda}_i \in \Lambda_i, i = 1, 2, \cdots, p$,

$$\begin{aligned} \bar{J}^*_{\mathscr{A}_i} &:= \bar{J}_{\mathscr{A}_i}(\bar{\lambda}_i^*, \bar{\lambda}_{-i}^*, \bar{\mu}^*) \le \bar{J}_{\mathscr{A}_i}(\bar{\lambda}_i, \bar{\lambda}_{-i}^*, \bar{\mu}^*), \\ \bar{J}^*_{\mathscr{N}} &:= \bar{J}_{\mathscr{N}}(\bar{\lambda}_i^*, \bar{\lambda}_{-i}^*, \bar{\mu}^*) \le \bar{J}_{\mathscr{N}}(\bar{\lambda}_i^*, \bar{\lambda}_{-i}^*, \bar{\mu}). \end{aligned}$$

A. Dynamic Case: Single Attacker

In the case where the network faces a single attacker, (7) is reduced to

$$\dot{z}(t) = -\lambda_1 z(t) + \mu. \tag{24}$$

Theorem 3: Consider the two-person node capturing game described by (24) and cost functions (23) and (22) with $p = 1$. Let $r_0 = r_1 := r$. Then, the open-loop Nash equilibrium solutions (λ_1^*, μ^*) of the two-person nonzero-sum game coincide with the open-loop saddle-point solutions (λ_1^S, μ^S) of the following two-person zero-sum game with dynamics (24) and the cost functional

$$L^2(\lambda_1, \mu) = \int_0^T (rz^2 + q_1 \lambda^2 - q_0 \mu^2) dt, \tag{25}$$

where the attacker minimizes L by choosing $\lambda_1^S(t) := \bar{\lambda}_1^S(t, z_0) \in \Lambda_1$, and the network maximizes it by choosing $\mu^S(t) := \bar{\mu}_1^S(t, z_0) \in \Gamma$.

Proof: The network aims to minimize (23), which is equivalent to maximizing

$$J_{\mathscr{N}}(\lambda_1,\mu)=\int_0^T (rz^2-q_0\mu^2+\xi_{\mathscr{N}}(\lambda_1))dt,$$

for any continuously differentiable function $\xi_{\mathscr{N}}$ of the attacker's control λ_1. Likewise, the attacker's goal is to minimize (22), which is equivalent to minimizing

$$J_{\mathscr{A}_1}(\lambda_1,\mu)=\int_0^T (rz^2+q_1\lambda_1^2+\xi_{\mathscr{A}_1}(\mu))dt,$$

for any continuously differentiable function $\xi_{\mathscr{A}_1}$ of the network's control μ. Let $\xi_{\mathscr{N}}(\lambda_1)=q_1\lambda_1^2$ and $\xi_{\mathscr{A}_1}(\mu)=-q_0\mu^2$. Then, we arrive at one single cost (or utility) functional of the game given by (25). Since the open-loop NE solution is independent of the state, finding the saddle-point solutions to the zero-sum game with cost functional (25) is equivalent to the nonzero-sum game. ∎

Note that the assumption that $r_0=r_1$ in Theorem 3 is made without loss of generality, as otherwise scaling would still lead to the same cost functionals.

Following the result in Theorem 3, we can conclude that the NE of the nonzero-sum game has the property of ordered interchangeability [19]. Hence, in the case of multiple equilibrium strategies, each player does not have to know (or guess) the particular strategy the other player will use in the game, since all such strategies are in equilibrium and yield the same value of the transformed (strategically equivalent) game.

B. Dynamic Case: Multiple Attackers

In the case of multiple attackers, we can characterize the OLNE of the $(p+1)$-person finite horizon differential game described by (7), (22) and (23) with the following necessary conditions.

Theorem 4: Consider the $(p+1)$-person node capturing game with multiple attackers described by (7), (22) and (23). If $\{\bar{\mu}^*,\bar{\lambda}_i^*,i=1,2,\cdots,p\},\bar{\lambda}_i^*\in\Lambda_i,\bar{\mu}^*\in\Gamma$ provides an open-loop Nash equilibrium solution, and $\{z^*(t),0\le t\le T\}$ is the corresponding state trajectory, then there exist $p+1$ costate functions $\phi_i,i=0,1,2,\cdots,p:[0,T]\to\mathbb{R}$, such that the following relations are satisfied:

$$\dot{z}^*(t) = -\left(\textstyle\sum_{i=1}^p \frac{\phi_i}{2q_i}\right)z^{2*}(t)-\frac{\phi_0}{2q_0},\ z^*(0)=z_0, \quad (26)$$

$$\dot{\phi}_i(t) = -2r_iz^*(t)+\phi_i\left(\textstyle\sum_{j=1}^p\lambda_j^*\right),\ \phi_i(T)=0, \quad (27)$$

$$\dot{\phi}_0(t) = 2r_0z^*(t)+\phi_0\left(\textstyle\sum_{j=1}^p\lambda_j^*\right),\ \phi_0(T)=0, \quad (28)$$

and the NE solutions need to satisfy for $i=1,2,\cdots,p$:

$$\lambda_i^*(t) := \bar{\lambda}_i^*(t,z_0)=\frac{\phi_iz^*}{2q_i}, \quad (29)$$

$$\mu^*(t) := \bar{\mu}^*(t,z_0)=-\frac{\phi_0}{2q_0}. \quad (30)$$

Proof: Following Theorem 6.11 in [19], we construct Hamiltonians for each player given by

$$H^0(t,\phi_0,z,\lambda_i,\lambda_{-i},\mu) := -r_0z^2+q_0\mu^2 +\phi_0\left(-\left(\sum_{i=1}^p\lambda_i\right)z(t)+\mu\right), \quad (31)$$

$$H^i(t,\phi_i,z,\lambda_i,\lambda_{-i},\mu) := r_iz^2+q_i\lambda_i^2 +\phi_i\left(-\left(\sum_{i=1}^p\lambda_i\right)z(t)+\mu\right) \quad (32)$$

$$i=1,2,\cdots,p.$$

By minimizing (31) with respect to μ and (32) with respect to λ_i, we arrive at unique solutions (29) and (30) due to the convexity with $q_i>0,i=0,1,\cdots,p$. In addition, the costate variables ϕ_i need to satisfy for $i=0,1,\cdots,p$:

$$\dot{\phi}_i=-\frac{\partial}{\partial z}H^i(t,\phi_i,z^*,\lambda_i^*,\lambda_{-i}^*,\mu^*).$$

Hence we arrive at (27) with terminal condition $\phi_i(T)=0$. ∎

Theorem 4 provides a set of necessary conditions for open-loop NE solutions to satisfy, and therefore it can be used to generate candidate solutions. It is also known that every such NE is weakly time-consistent [19]. Note that due to the nonnegativity constraint on the controls, we need $\phi_0\le 0$ and $\phi_iz\ge 0$. We will also require no conjugate points in the set of equations (26), (27), and (28). In order to see whether the candidate solution is the open-loop NE, we can apply sufficient conditions and check the convexity of $\hat{H}^i(t,\phi_i,\phi_{-i},z):=H^i(t,\phi_i,z,\lambda_i^*(\phi_i,z),\lambda_{-i}^*(\phi_{-i},z),\mu^*(z))$ with respect to z for $i=0,1,\cdots,p$. From (29), (30), (31) and (32), we obtain the following conditions for convexity

$$\frac{1}{2}\hat{H}_{zz}^0 = -r_0-\phi_0\left(\sum_{j=1}^p\frac{\phi_i}{2q_i}\right)\ge 0, \quad (33)$$

$$\frac{1}{2}\hat{H}_{zz}^i = r_i-\frac{\phi_i^2}{4q_i}+\phi_i\left(\sum_{j\ne i}\frac{\phi_j}{2q_j}\right)\ge 0. \quad (34)$$

If (33) and (34) are satisfied, we can conclude that for every given control of other players, the control of player i that satisfies (29), (30) yields an optimal path that satisfies the inequalities of Definition 2. Hence, (33) and (34) provide a sufficient condition for open-loop NE solutions.

In the case of two person game with one attacker, one can reduce (26), (27), (28) into

$$\dot{z}^*(t) = -\frac{\phi_1}{2q_1}z^{2*}(t)+\frac{\phi_0}{2q_0},\ z^*(0)=z_0, \quad (35)$$

$$\dot{\phi}_1(t) = -2r_1z^*(t)+\frac{\phi_1^2(t)z^*(t)}{2q_1},\ \phi_1(T)=0, \quad (36)$$

$$\dot{\phi}_0(t) = 2r_0z^*(t)+\frac{\phi_0\phi_1z^*(t)}{2q_1},\ \phi_0(T)=0. \quad (37)$$

Corollary 3: Consider the node capturing game with a single attacker and let $r_0=r_1$. If $\{\bar{\mu}^*,\bar{\lambda}_1^*\}$ provides an open-loop Nash equilibrium solution, then there exists one costate

function $\phi : [0,T] \to \mathbb{R}$, such that (35) and

$$\dot{\phi}(t) = -2r_1 z^*(t) + \frac{\phi^2(t) z^*(t)}{2q_1}, \ \phi(T) = 0,$$

with $\lambda_1^*(t) := \bar{\lambda}_1^*(t,z_0) = \frac{\phi z^*}{2q_1}$ and $\mu^*(t) := \bar{\mu}^*(t,z_0) = \frac{\phi}{2q_0}$.

Proof: The proof follows from (36), (37) and by noting that $-\phi_0(\cdot) = \phi_1(\cdot) := \phi(\cdot)$. ■

Note that Corollary 3 provides a set of necessary conditions that are equivalent to the zero-sum game described in Theorem 3. Let $r_0 = r_1 := r$. We can construct a single Hamiltonian $H = rz^2 + q_1\lambda_1^2 - q_0\mu^2 + \phi(-\lambda z + \mu)$ for the zero-sum game and arrive at the same set of conditions.

Theorem 5: The $(p+1)$-person finite-horizon open-loop differential game described by (7), (22) and (23) is equivalent to the following $(p+1)$-person game with a common cost functional

$$L^{p+1}(\lambda_1, \cdots, \lambda_p, \mu) = \int_0^T z^2 + \sum_{i=1}^{p} \bar{q}_i \lambda_i^2 - \bar{q}_0 \mu^2 dt,$$

where $\bar{q}_i = q_i/r_i, i = 0,1,\cdots,p$. The network maximizes L^{p+1} by choosing $\mu^S(t) := \bar{\mu}_1^S(t,z_0) \in \Gamma$, and attacker $\mathscr{A}_i, i = 1,2,\cdots,p$, minimizes it by choosing $\lambda_i^S(t) := \bar{\lambda}_i^S(t,z_0) \in \Lambda_i$.

Proof: The proof follows the similar argument as in Theorem 3 and by scaling the cost functionals with r_i we can form L^{p+1} in the same way as in Theorem 3 for $(p+1)$-person game. ■

Note that Theorem 5 shows equivalence of the open-loop NE of the $(p+1)$-person game to the saddle-point solution of a two-player team game where the minimizing player is actually a team of p players. The equilibrium strategies from the $(p+1)$-person zero-sum game coincide with the one studied in Theorem 4. We can also verify this by noting that the adjoint equations (36) are symmetric if $r_i = r$, and ϕ_0 is opposite in sign with other ϕ_i in (37).

VI. NUMERICAL STUDIES

In this section, we illustrate with numerical examples the NE solutions for the node capture and cloning games for both the static and the dynamic cases.

A. Static Case Simulations

For a single attacker, we analyze the two cases in Theorem 1. For case (i), we let $k_0 = 3/10$, and $k_1 = 1/2$, which yields the NE of $u^* = 3/10$ and $\lambda_1^* = 1$. The steady-state value is $z_{ss} = 0.231$. For case (ii), we let $k_0 = 7/10$, and $k_1 = 2/5$, which yields $u^* = 1$, $\lambda_1^* = 2/5$, and $z_{ss} = 0.714$.

For two attackers, we analyze the two cases in Corollary 1 and Corollary 2. For Cor. 1, we let $k_0 = k_1 = k_2 = 3/5$, which yields the NE of $u^* = 3/10$ and $\lambda_1^* = \lambda_2^* = 1$. The steady-state value is $z_{ss} = 0.231$. For Cor. 2, we let $k_1 = k_2 = 2/5$, and $k_0 = 4/5$, which yields $u^* = 4/5$, $\lambda_1^* = \lambda_2^* = 1/2$, and $z_{ss} = 0.615$.

B. Dynamic Case Simulations

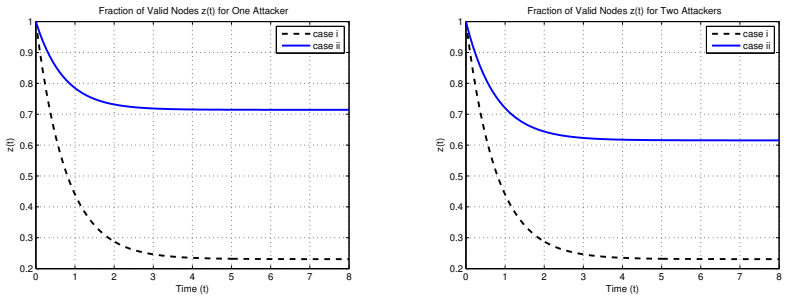
In the single attacker case, we set $r_0 = r_1 = 1$ and $q_0 = 1, q_1 = 2/3$. Fig. 3(a) shows the strategies of the attacker and the network in the two-person game, and in Fig. 3(b) shows the trajectory of the state variable $z(t)$ and costate variable $\phi(t) = \phi_1(t) = -\phi_0(t)$. Under the equilibrium strategies λ_1^* and μ^*, the state variable $z(t) = 1 - x(t)$ reaches its steady state $z_{ss} = 0.818$ within $t \in [0,3]$. The attacker constantly spends more control effort capturing the nodes in the network than the network's effort to recover the nodes.

For two attackers we set $r_0 = 1, r_1 = 1.5, r_2 = 1.2$ and $q_0 = q_1 = q_2 = 1$. We observe that attacker $\mathscr{A}_2$ is more malicious than attacker $\mathscr{A}_1$ since it places higher weights on the state variable $z(t)$. The open-loop NE strategies will be equivalent to the case where all $r_i = 1$ for $i = 0,1,2$ and $q_0 = 1, q_1 = 2/3, q_2 = 5/6$. In Fig. 3(d), we show the trajectory of state variable $z(t)$ and costate variables ϕ_0, ϕ_1, ϕ_2 at open-loop NE, and in Fig. 3(c), we show the strategies of the attackers and the network. We see from Fig. 3(d) that at the NE, the network reaches its steady state $z_{ss} = 0.612$. Attacker $\mathscr{A}_1$ constantly uses more control effort to compromise the network than attacker $\mathscr{A}_2$ due to attacker $\mathscr{A}_1$'s higher level of malicious intent.

In the example of the single attacker, we see that attacker $\mathscr{A}_1$ alone can cause harm to the network and let the network reach $z_{ss}^2 = 0.818$ with maximum effort at $t = 0$ given by $\lambda_{1,\max} = 1.22$. On the other hand, in the case where attacker $\mathscr{A}_2$ is the single attacker in the network, the network reaches $z_{ss}^2 = 0.914$ under NE, and the maximum effort over time occurs also at $t = 0$ given by $\lambda_{2,\max} = 1.091$. We observe that the consequence of having two attackers in the network is more severe than the sum of damages caused by attackers individually. The steady state value $z_{ss} = 0.612 < \bar{z}_{ss} := 1 - \Delta z_{ss}^1 - \Delta z_{ss}^2 = 0.732$, where $\Delta z_{ss}^1 := 1 - z_{ss}^1 = 0.182$, and $\Delta z_{ss}^2 := 1 - z_{ss}^2 = 0.086$. In addition, the attackers tend to use less effort when more attackers are present in the network. The maximum efforts of attackers $\mathscr{A}_1$ and $\mathscr{A}_2$ are 0.910 and 0.728, respectively, in the two attacker case.

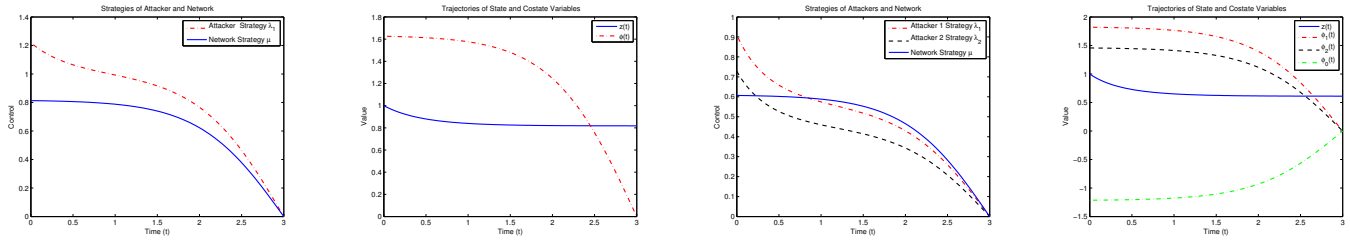
VII. CONCLUSION

In this paper, we have studied the problem of node capture and cloning attacks on wireless sensor networks with multiple attackers. We have formulated a game-theoretic framework to model the strategic behaviors between the network and the group of attackers. We have considered two game scenarios: one is static and the other one is dynamic. In both cases, the network determines revocation rates to protect the system, whereas the attackers choose individual capture rates to compromise the network operation. In the static case, the capture rate has been taken as a time-invariant parameter, and the revocation rate as a linear function of the state. We have derived explicit functions of time for both rates and proved the existence of pure-strategy Nash equilibria. In the dynamic case, the capture rates and revocation are general functions of time. We have studied the open-loop Nash equilibrium of the game and have characterized the equilibrium solutions with a set of necessary conditions. In



(a) (b)

Fig. 4. Static case: (a) the fraction of valid nodes left in the network, $z(t)$, for one attacker, (b) $z(t)$ for two attackers.



(a) (b) (c) (d)

Fig. 5. Dynamic case: (a) the strategies of one attacker, (b) the trajectory of the state variable $z(t)$ and costate variable $\phi(t) = \phi_1(t) = -\phi_0(t)$ for one attacker, (c) the strategies of two attackers, and (d) the trajectory of the state variable $z(t)$ and costate variables $\phi_0(t), \phi_1(t), \phi_2(t)$ for two attackers.

addition, we have shown the equivalence of the $(p+1)$-person nonzero-sum dynamic game to a zero-sum game between the network and the attackers lumped together as a team.

As future work, we intend to study the dynamic game under different information structures, which includes the one under feedback strategies for both players, incomplete information games, and games with mixed information structures. It is also of interest to investigate topological features of wireless sensor networks and analyze their effects on node capture and cloning attacks. We also intend to consider different structures of the cost functions by extending the quadratic costs to a more general form of costs.

REFERENCES

[1] A. Milenkovic, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications*, vol. 29, no. 13-14, pp. 2521–2533, 2006.

[2] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," *Proc. 1st ACM International Workshop on Wireless Sensor Networks and Applications*, pp. 88–97, 2002.

[3] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proc. 9th ACM Conference on Computer and Communications Security*, pp. 41–47, 2002.

[4] B. Parno, A. Perrig, and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," *Proc. IEEE Symposium on Security and Privacy*, pp. 49–63, 2005.

[5] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[6] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[7] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: A system theoretic approach," *Proc. 49th IEEE Conference on Decision and Control*, pp. 6765–6772, 2010.

[8] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 80–89, 2007.

[9] Z. Li and G. Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," *Proc.6th International IEEE Conference on Mobile Adhoc and Sensor Systems*, pp. 1030–1035, 2009.

[10] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Survey*, September 2013.

[11] T. Alpcan and T. Başar, *Network Security: A Decision and Game Theoretic Approach*, Cambridge University Press, January 2011.

[12] E. Altman, T. Başar, and V. Kavitha, "Adversarial control in a delay tolerant network," *Decision and Game Theory for Security*, T. Alpcan, L. Buttyan, and J. Baras (Eds.): GameSec 2010, LNCS 6442, pp. 87–106, 2010.

[13] Q. Zhu, H. Li, Z. Han and T. Başar, "A stochastic game model for jamming in multi-channel cognitive radio systems," in *Proc. of IEEE International Communications Conference (ICC)*, pp. 1–6, 2010.

[14] Q. Zhu, W. Saad, Z. Han, H. V. Poor and T. Başar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach" *Proc. of IEEE Military Communications Conference (MILCOM)*, pp. 119–124, 2011.

[15] Y. Mo, E. Garone, A. Casavola and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," *Proc. IEEE Conference on Decision and Control*, pp. 5967–5972, 2010.

[16] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," *Proc. 49th IEEE Conference on Decision and Control*, pp. 5991–5998, 2010.

[17] Q. Zhu and T. Başar, "Toward robust and resilient control design for cyber-physical systems with an application to power systems," *Proc. 50th IEEE Conference on Decision and Control and European Control Conference*, pp. 4066-4072, 2011.

[18] K. C. Border, *Fixed Point Theorems with Applications to Economics and Game Theory*, Cambridge University Press, 1985.

[19] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, SIAM Series in Classics in Applied Mathematics, Philadelphia, January 1999.

[20] T. Başar and P. Bernhard, *H-infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*, Birkhäuser, Boston, MA, August 1995.