Node Capture Attacks in Wireless Sensor Networks: A System Theoretic Approach

Tamara Bonaci, Linda Bushnell and Radha Poovendran

***Abstract*— In this paper we address the problem of physical node capture attacks in wireless sensor networks and provide a control theoretic framework to model physical node capture, cloned node detection and revocation of compromised nodes. By combining probabilistic analysis of logical key graphs and linear control theory, we derive a dynamical model that efficiently describes network behavior under attack. Using LQR and LQG optimal control theory tools, we develop a network response strategy, which guarantees secure network connectivity and stability under attack. Detailed simulations are presented to validate the methodology.**

I. INTRODUCTION

Wireless sensor networks (WSN) are increasingly becoming the networks of choice in industrial, medical and military applications, including remote plant control, health monitoring and target surveillance. A typical WSN consists of a large number of sensor nodes randomly deployed over a wide area. It is expected to operate unattended over a long period of time, with a minimal interference of central authority. Sensor nodes are typically low-cost hardware components with severe limitations on energy, memory and communication resources. Thus, nodes have to collaboratively establish and maintain one-hop and multi-hop end-to-end network connectivity.

Due to the broadcast nature of the transmission media they use, WSNs are vulnerable to various security attacks, such as eavesdropping [1], jamming [2] and node capture attacks [3].

Eavesdropping attacks in WSNs can be prevented by making use of symmetric key based cryptographic techniques to control access to communication among sensor nodes. The use of cryptography, however, requires a mechanism to generate, distribute and when needed, revoke and refresh cryptographic keys used for secure communication. An efficient and practical key assignment method for large scale WSNs, using random graph techniques was presented in [4]. This probabilistic key assignment technique essentially exploits the property that due to radio range limitations of sensors, keys can be reused to establish secure links by many pairs of nodes.

Capturing a node enables an adversary not only to get ahold of cryptographic keys and protocol states, but also to clone and redeploy malicious nodes in the network. As pointed out in [3], the existing adversarial models such as Byzantine failure or Dolev-Yao threat models are inadequate to describe node capture attacks. Furthermore, at present there does not exist any other adversarial model in the literature to describe node capture attacks.

Despite the lack of a security threat model, in recent years, efforts have been made to understand and mitigate node capture and cloning attacks. In [4], the authors present a probabilistic key predistribution method that allows secure deployment of WSNs. They also present node revocation and keys update techniques to ensure network connectivity and service. Efficient methods to identify cloned nodes in the network are described in [3]. Still, the lack of a common analytical framework prevents any discussion about the degree of an attack, the network's resilience against an attack and the stability of WSNs, all of which are required to guarantee secure and reliable WSNs.

In this paper, we present such a comprehensive framework based on control theory for the case when there is a node capture attack. Our framework is simultaneously able to incorporate secure deployment techniques, corrupted nodes identification algorithms and node revocation methods in order to study WSNs' resilience to node capture attacks. In addition, our framework enables stability and performance analysis of WSNs under attack.

We make the following contributions:

- We develop a control-theoretic framework to address the problem of node capture attacks in a WSN, by mapping the network security problem into a control theory problem.
- We derive a linear dynamical model for a WSN under node capture attacks, where all of the model parameters are completely characterized in terms of the network parameters.
- We derive different controllers in order to control the network response to node capture attacks. The network response strategies are based on the stability theory of linear systems and optimal control theory methods, specifically the Linear Quadratic Regulator (LQR) and Linear Quadratic Gaussian (LQG) methods.
- Using the proposed framework, we simulate and analyze the network performance and stability under node capture attacks.

The paper is organized as follows: in Section II, we present models of an adversary and a WSN and state the necessary assumptions. In Section III, we show the mapping from network security into a control theory framework and introduce the dynamical model of a WSN under node capture attacks. In Section IV, we propose different network responses to node capture attacks using the stability theory of linear systems and LQ optimal control theory. In Section V, we

T. Bonaci and R. Poovendran are with the Network Security Lab (NSL), Electrical Engineering Department, University of Washington, Seattle, WA, 98195, USA. Email: {tbonaci, rp3}@u.washington.edu

L. Bushnell is with the Networked Control System Lab (NCS), Electrical Engineering Department, University of Washington, Seattle, WA, 98195, USA. Email: lb2@u.washington.edu

TABLE I

A SUMMARY OF NOTATION USED

Symbol	Definition
$\mathcal{N}$	Set of sensor nodes deployed in the network
N	Number of nodes in the network
M	Number of nodes needed to be captured in order to compromise all the links in a WSN
$\mathcal{C}$	Set of compromised nodes
P	Size of the key pool
$\mathcal{K}_t$	Set of symmetric cryptographic keys at time t
$\mathcal{K}_{t,n_i}$	Set of keys held by the valid node n_i at time t
$\mathcal{K}_{t,n_i \cap n_j}$	Keys nodes n_i and n_j have in common at time t
K	Number of distinct keys assigned to each node
$\mathcal{K}_{t\mathcal{C}}$	Set of keys held by compromised nodes at time t
$\mathcal{K}_{t,c_k}$	Set of keys held by the compromised node c_k at time t
λ	Node capture rate
$x(t)$	Number of compromised nodes at time t
ω_n	Number of cloned nodes deployed in the network
γ	Detection rate
$y(t)$	Number of nodes with all keys compromised at time t
ω_α	Number of valid nodes with all keys compromised
μ	Revocation rate
$\tilde{R}$	Cost of revocation and secure update of the keys held by the revoked node, ($R = \tilde{R}^2$)
$\tilde{Q}$	Cost reflecting the impact a compromised node has on network connectivity, ($Q = \tilde{Q}^2$)
J	Cost of control action
$\bar{u}(t)$	Optimal control signal
u_{ff}	Static feedforward signal
S	Solution of the controller ARE
S_f	Solution of the filter ARE
Θ_n	Covariance of the process noise ω_n
Θ_α	Covariance of the measurement noise ω_α
K_f	Kalman gain

present simulation results and analyze network performance when different control approaches are used. In Section VI, we conclude the paper.

II. BACKGROUND AND PRELIMINARIES

In this section, we state the assumptions about the system to be controlled and an adversary performing an attack. A summary of the notation used is provided in Table I.

A. Network Model

We assume WSNs use encrypted communication with key assignment based on the random key predistribution scheme. Each node is randomly assigned a set of K different keys from a key pool of P keys defined for a particular sensor network [4]. Two sensor nodes are able to securely communicate if they share at least one common key.

We let $\mathcal{N}$ denote a set of N sensor nodes deployed in a WSN and $\mathcal{K}_t$ a set of symmetric cryptographic keys used for secure communication in a WSN at time t. Then a WSN can be represented as a random graph $G(\mathcal{N}, \mathcal{K}_t)$, where a set of vertices $\mathcal{N}$ represents sensor nodes deployed in a WSN and a set of edges $\mathcal{K}_t$ represents secure communication links at time t. Each node $n_i \in \mathcal{N}, i \neq j$ is assigned a set of keys $\mathcal{K}_{t,n_i}$. A pair of nodes $n_i, n_j \in \mathcal{N}$ can communicate securely if and only if they share at least one common key, i.e., if $\mathcal{K}_{t,n_i} \bigcap \mathcal{K}_{t,n_j} \neq \emptyset$.

Let $\mathcal{C}$ denote a set of captured nodes. If there exist a node $c_k \in \mathcal{C}$, a set of keys $\mathcal{K}_{t,c_k}$ held by node c_k is considered to be compromised. Due to the key distribution scheme used, secure links between any two nodes $n_i, n_j \in \mathcal{N}$ using a key $k_i \in \mathcal{K}_{t,c_k}$ are considered to be exposed to an adversary and therefore insecure.

B. Network Administrative Assumptions

We assume the owner of a WSN is able to perform the following administrative actions: detection of compromised as well as cloned nodes, revocation and replenishment of nodes and revocation and secure update of cryptographic keys.

Due to a limited lifetime, cryptographic keys in WSNs can expire. Therefore, keys used for secure communication in WSNs should be periodically updated. Keys must also be updated if they are exposed or compromised. Compromised keys must be revoked and all the valid nodes that used compromised keys must be securely updated with freshly generated keys.

Ideally, all the compromised and cloned nodes should be detected and revoked, along with the keys held by them. In practice, however, there is a non-zero probability that some valid nodes will be detected as compromised (false alarms), and some compromised nodes will not be detected (misdetection). Even though a perfect detection may not possible, in this work we assume an intelligent detection algorithm that minimizes the number of false alarms and misdetections while maximizing the probability of compromised detection is used. When a detection algorithm identifies a node as compromised or cloned, the node as well as the keys held by that node, are placed on a revocation list. All the valid nodes sharing keys with the revoked node are updated with freshly generated keys in order to maintain connectivity.

Finally, even in the absence of any adversarial action, some network nodes may fail and have to be replaced with new nodes possessing suitable uncompromised keys to establish secured links with the remaining network nodes.

C. Adversarial Model

We consider a set of multiple adversaries, acting collaboratively within the deployment area $\mathcal{A}$. Each adversary is assumed to have limited resources and mobility.

Each adversary is able to capture a sensor node, steal all the information stored within the captured node, such as cryptographic keys and measured data, and use the compromised keys to actively listen on any of the exposed links. In addition, adversaries are capable of functionally cloning a captured node and collaboratively deploying them in the WSN.

The goal of such a collaborative set of adversaries is to capture enough nodes to be able to listen on all the exposed

links or gather all the distinct keys assigned to nodes in the WSN[1] in order to gain control of the WSN.

III. Linear System Model

In this section, we define the parameters and variables needed to model a WSN under node capture attacks.

A. Problem Mapping

Consider an adversary mounting a node capture attack on a WSN with M sensor nodes being what the adversary needs to capture to compromise all of the links or all of the cryptographic keys assigned to the network. At a time unit t, due to limited resources, the adversary is able to capture only a subset of nodes. We define parameter λ as the average rate at which the adversary captures sensor nodes in one time unit and refer to it as the *node capture rate.*In addition, the adversary is able to deploy a certain number of cloned nodes into a WSN. We denote the number of cloned nodes an adversary deploys in a WSN in one time unit as the parameter ω_n. It is a random variable whose value is known to be $\omega_n \ll M$ due to the fact that an adversary does not want to draw any attention to his activities ("stealthy behavior"). We denote $x(t)$ as the number of compromised nodes in a WSN at time unit t.

Each compromised node $c_i \in \mathcal{C}$ holds a set of K distinct cryptographic keys. Due to the fact that keys are being reused in a WSN, there exists a non-zero probability that the union of the sets of keys held by all the compromised nodes $\mathcal{K}_{t\mathcal{C}}$ completely covers the set of keys assigned to one or more valid nodes $n_i \in \mathcal{N}$. Valid nodes with all the keys compromised are not able to securely communicate. The parameter ω_α represents the number of valid nodes $n_i \in \mathcal{N}$ with all the keys compromised. It is a random variable, whose value is known to be $\omega_\alpha \ll M$.

Each time compromised detection is performed, due to the imperfections in the detection algorithm (false alarms and misdetections) only a subset of nodes with all of their keys compromised can be detected. We define a subset of nodes that are actually detected as $\gamma x(t)$, where the parameter γ denotes the *detection rate.*We use the parameter $y(t)$ to denote the number of detected nodes with all keys compromised.

We define the parameter μ as the *minimum revocation rate* required to guarantee secure connectivity to all the valid nodes under node capture attacks, where compromised nodes are detected using an intelligent, yet imperfect algorithm.

Thus, the processes in a WSN under node capture attacks can be modeled using the following equations[2]:

$$\begin{aligned} \dot{x}(t) &= \lambda[M - x(t)] - \mu x(t) + \omega_n \\ y(t) &= \gamma x(t) + \omega_\alpha(t) \end{aligned} \tag{1}$$

[1]Note that, due to the fact that two nodes need to be within each other's radio range and need to share at least one common key, in order to be able to communicate, it is possible that the number of keys assigned to sensor nodes in the WSN exceeds the number of keys used within the WSN.

[2]Due to the assumption that multiple adversaries are collaboratively mounting an attack, we note that the node capture rate λ can scale with increase/decrease in the parameter M, the number of nodes that need to be captured.

Equation (1) is a mathematical representation of the physical system, showing how the number of compromised nodes changes in each time unit due to adversarial and WSN's administrative activities. It represents a mapping between the network security problem and a linear dynamical system.

B. State-space Representation

The linear dynamic mapping of a WSN under node capture attacks (1) can be represented in the standard state-space form:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + \xi_n(t) \\ y(t) &= Cx(t) + Du(t) + \nu(t) \end{aligned} \tag{2}$$

by defining the process noise and the measurement noise as:

$$\begin{aligned} \xi_n(t) &= \lambda M + \omega_n \\ \nu(t) &= \omega_\alpha \end{aligned}$$

and the state-space matrices as:

$$A = -\lambda,\ B = 1,\ C = \gamma \text{ and } D = 0$$

Thus, we have single-input, single-output (SISO) linear dynamical system[3]:

$$\begin{aligned} \dot{x}(t) &= -\lambda x(t) - \mu x(t) + (\lambda M + \omega_n) \\ y(t) &= \gamma x(t) + \omega_\alpha \end{aligned} \tag{3}$$

where the control input $u(t) := -\mu x(t)$ represents a proportional controller with the proportional gain μ.

IV. Developing an optimal feedback response

A WSN under node capture attacks incurs two different costs: a cost of having compromised nodes in the network and a cost of revoking compromised nodes. We define the average cost of revoking one compromised node as $\tilde{R}$ and the cost of having one compromised node in the network as $\tilde{Q}$. Both costs can be completely characterized in terms of network parameters by analyzing the logical key graph associated with the WSN. We make the observation that the unit cost of having compromised node c_k in the network, $\tilde{Q}$, reflects the impact of the node c_k on network connectivity. Thus, when communication in a WSN is secured using a general probabilistic key predistribution scheme [4], we can express the cost $\tilde{Q}$ (maximum and average) as follows:[4]

$$\tilde{Q}_{max} = \tfrac{N\cdot(N-1)K^3}{40P^2} \tag{4a}$$

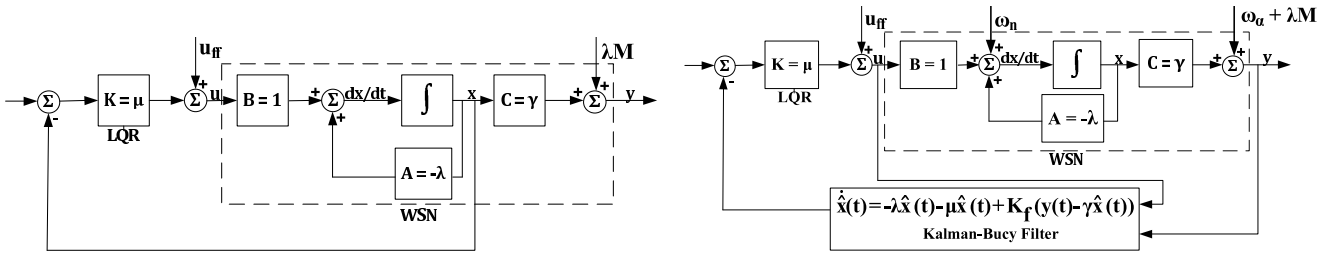
$$\tilde{Q}_{avg} = \tfrac{N\cdot(N-1)\cdot p}{40}\left\{1 - \left[1 - \left(\tfrac{K}{P}\right)\tfrac{N\left(\frac{K}{P}\right)-1}{N-1}\right]^K\right\} \tag{4b}$$

where p represents the probability that any two nodes in the WSN share a link.

The cost $\tilde{R}$ can be expressed similarly by noting that the revocation cost reflects the communication cost caused by

[3]The given linear SISO model is a queueing theory representation of the network security problem.

[4]See the Appendix for the derivation of costs $\tilde{Q}$ and $\tilde{R}$.



(a) (b)

Fig. 1. Model mapping of the WSN parameters under node capture attacks: state variable $x(t)$, representing the number of captured nodes, output variable $y(t)$, representing the number of nodes with all keys compromised, feedback control signal $u(t) = -\mu x(t)$, where control parameter μ denotes the minimum revocation rate needed, u_{ff} static feedforward control signal, process noise ω_n, representing the number of cloned nodes, measurement noise ω_α, representing the number of valid nodes with all the keys compromised, matrices $A = -\lambda$, where λ denotes the node capture rate, $B = 1$, $C = \gamma$, where γ denotes the detection rate, (a) State-space model with LQR controller (noise signals ignored), (b) State-space model with LQG controller (Gaussian approximation of noise signals).

refreshing the keys that valid nodes shared with the captured node (linear and logarithmic form of $\tilde{R}$):

$$\tilde{R}_{lin} = \frac{K^2 N}{P} \quad (5a)$$

$$\tilde{R}_{log} = K \log \frac{KN}{P} \quad (5b)$$

By letting $Q = \tilde{Q}^2$ and $R = \tilde{R}^2$, we define a quadratic performance measure J, referred to as the *cost of control action* as follows:

$$J = \int_0^\infty [(x(\tau)^T Q x(\tau) + u(\tau) R u(\tau)] d\tau \quad (6)$$

The controller design goal is to find an optimal revocation rate μ, such that in a finite number of time units all of the compromised nodes are revoked from the WSN, in addition to minimizing the cost of control action $J(t)$. There exist many control theoretic methods for achieving this goal; we investigate two different methods based on LQR and LQG optimal control theory methods.

A. The Optimal LQR Network Response

In order to use LQR theory, we first need to understand the noise terms ω_n and ω_α in the system equation (3). We observe that the process noise is defined as a sum of a constant noise term λM and a random noise term ω_n. Since the random noise signal ω_n is assumed to be much smaller than M, it can be disregarded. We then observe that the output signal $y(t)$ is equal to the sum of the state variable $\gamma x(t)$ and a random noise term ω_α. Again, since the random noise signal ω_α is assumed to be much smaller than M, it can be disregarded.

Our linear system (3) now becomes (Figure 1(a)):

$$\begin{aligned} \dot{x}(t) &= -\lambda x(t) - \mu x(t) + \lambda M \\ y(t) &= \gamma x(t) \end{aligned} \quad (7)$$

The problem of finding the optimal revocation rate μ is equivalent to the problem of disturbance rejection in the sense of LQR optimal control theory where the disturbance for our system is λM. This problem can be solved in two steps. We first find a constant feedforward signal u_{ff} that maps the system (7) into a system without disturbance (disturbance rejection) and then we find an optimal LQR control input $-\mu x(t)$ for the disturbance-free system. Therefore, we define a new disturbance-rejection controller $\bar{u}(t)$ as [5]:

$$\bar{u}(t) = -\mu x(t) + u_{ff} \quad (8)$$

where the term $-\mu x(t)$ represents a dynamical feedback control signal that is used to control the revocation action in a WSN. The term u_{ff}, a static feedforward control signal, represents the subset of sensor nodes in a WSN whose cryptographic keys should be automatically refreshed in one time unit, due to the fact that an adversary is expected to capture λM nodes in each time unit.

Theorem 1: There exists a unique optimal control signal $\bar{u}(t)$ that asymptotically stabilizes the system (7).

Proof: The dynamical feedback signal $-\mu x(t)$ represents the output of the proportional LQR controller for the disturbance-free system, with the optimal proportional gain μ:

$$\mu := \frac{S}{R} \quad (9)$$

where S represents the solution of the equation:

$$\frac{1}{R} S^2 + 2\lambda S - Q = 0 \quad (10)$$

which is a scalar representation of the Algebraic Riccati Equation (ARE):

$$A^T S + S^T A + Q - S B R^{-1} B^T S = 0 \quad (11)$$

Note that the positive solution to (10) is:

$$S = \lambda R \left(-1 + \sqrt{1 + \frac{Q}{R} \frac{1}{\lambda^2}} \right) \quad (12)$$

The static feedforward control signal u_{ff} used to reject the constant disturbance λM is defined as $u_{ff} := -\frac{\lambda M}{R} b$, where parameter b represents the solution of the equation:

$$\left(\lambda + \frac{S}{R} \right) b - \lambda M S = 0 \implies b = \frac{\lambda M S}{\lambda + \mu} \quad (13)$$

By LQ control theory, since there exists positive solution S of the ARE (10) and constant feedforward signal u_{ff}, the

control signal $\bar{u}(t)$ asymptotically stabilizes the system (7). ■

Remark 1: From Theorem 1 it follows that for a given triplet (λ, Q, R) there always exists a unique optimal asymptotically stable revocation rate μ. Therefore, if we would decide to put the static feedforward signal $u_{ff} = 0$, the dynamic feedforward signal $-\mu x(t)$ would still be able to stabilize the system (7), but there would exist a steady-state error $e_{ss} = \lambda M$.

Remark 2: An important consequence of the asymptotic stability of control signal $\bar{u}(t)$ is that it guarantees that a WSN will always stay connected, i.e., an adversary will never be able to compromise enough keys to disrupt network connectivity as long as the adversary's actions were described reliably by capture rate λ. Even more, if the captured nodes would not be detected immediately and administrative actions would start only after there are $x(0) < M$ compromised nodes in the network, due to the asymptotic stability of the control signal $\bar{u}(t)$, all the captured nodes would still be revoked, while the cost of the control action would stay minimal.

Remark 3: From equations (9) and (12), we can express the revocation rate as $\mu = \lambda\left(-1+\sqrt{1+\frac{Q}{R}\frac{1}{\lambda^2}}\right)$. Due to the fact that both costs Q and R can be expressed as functions of network parameters $f(N, K, P)$, using equations (4a) and (5a) we can also express μ as a function of network parameters, $\mu = \lambda\left[-1+\sqrt{1+\frac{1}{\lambda^2}\frac{(N-1)^2K^2}{1600P^2}}\right]$.

B. The Optimal LQG Network Response

Instead of disregarding the random noise terms ω_n and ω_α in equation (3), we assume these noise terms are uncorrelated zero-mean, normally distributed random variables $\mathcal{N}(0, 1)$. The output signal $y(t)$, representing the number of nodes with all keys compromised, now becomes corrupted with the Gaussian random variable ω_α. Therefore, in order to find the optimal control signal $u(t)$, we first need to find the estimate $\hat{y}(t)$ of the corrupted output signal $y(t)$.

The problem of finding the optimal revocation rate μ now becomes equivalent to the problem of disturbance rejection in sense of LQG control theory (Figure 1(b)).

The optimal LQG controller design problem can be solved by first finding an optimal state estimator (LQE problem) and then solving the disturbance-rejection problem with estimated output signal $\hat{y}(t)$ (LQR problem). The separation principle [5] guarantees that the dynamic LQG controller, found by separately solving LQE and LQR problems, will stabilize the system (3) as long as both the optimal state estimator and optimal LQR controller are asymptotically stable.

Theorem 2: There exists a unique optimal asymptotically stable state estimator (Kalman-Bucy filter, with Kalman gain K_f) for the system (3).

Proof: Let $\hat{x}(t)$ denote the estimated value of compromised nodes $x(t)$ and $e(t) := x(t) - \hat{x}(t)$ the estimation error. The estimator design goal is to find an estimator that minimizes the estimation mean-squared error V_f:

$$V_f = \lim_{t\to\infty} \mathbb{E}[e^2(t)] \tag{14}$$

and has the following form:

$$\dot{\hat{x}}(t) = -\lambda\hat{x}(t) - \mu\hat{x}(t) + K_f[y(t) - \gamma\hat{x}(t)] \tag{15}$$

where $K_f[y(t) - \gamma\hat{x}(t)]$ represents the correction term that is used to ensure the estimation error is bounded.

For the linear dynamical system with Gaussian noise (3), the problem of finding the optimal state estimator is equivalent to the LQR problem [5], where instead of the pair (A, B) = ($-\lambda$, 1) in equation (11), we use the pair (A^T, C^T) = ($-\lambda$, γ) and instead of costs Q and R we use the covariances Θ_n and Θ_α, defined as $\mathbb{E}[\omega_n(t)\omega_n(\tau)] = \Theta_n\delta(t-\tau)$, $\mathbb{E}[\omega_\alpha(t)\omega_\alpha(\tau)] = \Theta_\alpha\delta(t-\tau)$. Thus, the optimal Kalman gain is defined as [5] $K_f := \frac{S_f\gamma}{\Theta_\alpha}$ where S_f represents the solution of the filter ARE:

$$\frac{\gamma^2}{\Theta_\alpha}S_f^2 + 2\lambda S_f - \Theta_n = 0 \tag{16}$$

Equation (16) is a scalar representation of the ARE (11), with the positive solution:

$$S_f = \lambda\Theta_\alpha\left(-1+\sqrt{1+\frac{\Theta_n}{\Theta_{\alpha^2}}\frac{\gamma^2}{\lambda^2}}\right) \tag{17}$$

It is known from linear quadratic control theory that there exists a unique optimal asymptotically stable proportional gain K_f if there exist a unique positive-definite solution S_f to the ARE (16). ■

Theorem 3: There exists an optimal dynamic LQG controller that stabilizes the system (3).

Proof: In Theorem 2 we showed that there exists an optimal asymptotically stable Kalman-Bucy filter for the system (3). We use methods of Section IV A with the estimated state variable $\hat{x}(t)$ in order to design an LQR controller with control signal $\bar{u}(t) = (-\mu\hat{x}(t) + u_{ff})$. As shown in Section IV A, such a control signal $\bar{u}(t)$ is optimal and asymptotically stable. Therefore, by separation principle [5], there exists an optimal dynamic LQG controller that stabilizes the system (3). ■

Remark 4: There are two important consequences of the stability result. First, it means that the WSN's owner will be able to revoke all of the compromised nodes, even if an adversary deploys a subset of cloned nodes in the network. Second, it means that the network will remain connected even in the case where there exists a subset of valid nodes in the network, whose keys are all compromised.

V. Simulation results and performance analysis

In this section we provide simulation results and analyze the WSN's behavior under node capture attacks. Due to the assumption that cryptographic keys in WSNs are assigned using the random key predistribution scheme [4], we are able to derive the direct relationship between the costs Q and R, and the network parameters N, K, P (see Appendix).

We analyze the behavior of four different WSNs, with the network parameters given in Table II. The adversary's capture rate is set to λ = 0.05 and detection rate to γ = 1. Noise signals ω_n and ω_α are set to $\mathcal{N}(0, 10)$ for simulation purposes, however they can both be characterized as functions of network parameters. The process noise ω_n can be characterized by analyzing the adversary's strategy of avoiding detection of cloned nodes.[5]

The measurement noise ω_α is shown to follow the binomial probability distribution $\mathcal{B}([N - x(t)], p^*)$, where $p^* = \left(1 - \left[\frac{N-\beta_i}{N-1}\right]^{x(t)}\right)^K$ denotes the probability that all of the keys of the valid node $n_i \in \mathcal{N}$ are compromised [6]. By the Central Limit Theorem ω_α can be approximated as $\hat{\omega}_\alpha \sim \mathcal{N}(0, 1)$, with

$$\hat{\omega}_\alpha = \frac{\omega_\alpha - \{[N - x(t)]p^*\}}{\sqrt{N - x(t)}\sqrt{[N - x(t)]p^*(1 - p^*)}}$$

From the logical key graph perspective, the state variable $x(t)$ is a random variable and it introduces randomness in variables ω_α and $\hat{\omega}_\alpha$.

In order to simulate the system (3), we need to calculate the number of nodes, M, an adversary needs to capture to disrupt network connectivity. By noting that the process of assigning the key $k_i \in \mathcal{K}_t$ can be modeled as a binary switch process, we can calculate the probability that the key k_i is not assigned to any node as:

$$\mathbb{P}[\text{key } k_i \text{ is not assigned to any node}] = \left(1 - \frac{K}{P}\right)^N \quad (18)$$

Using equation (18), the expected number of keys assigned to one or more nodes can be calculated as: $\mathbb{E}[K_{asg}] = P \cdot \mathbb{E}[\text{key } k_i \text{ assigned}] = P \cdot \left[1 - \left(1 - \frac{K}{P}\right)^N\right]$ Under the assumption that there exists a subset of nodes $\mathcal{N}_{max} \in \mathcal{N}$ in the WSN such that any two nodes n_i and $n_j \in \mathcal{N}_{max}$ do not share a key (maximum non-overlapping set of nodes), we define the number of nodes an adversary needs to capture as: $M = \frac{P}{K}\left[1 - \left(1 - \frac{K}{P}\right)^N\right]$.

Table II shows the calculated parameter M as well as costs R_{lin}, R_{log}, Q_{max} and Q_{avg}, where R_{lin} denotes the revocation cost using a linear-update method (5a), R_{log} the revocation cost using a tree-structure update (5b), Q_{max} the maximum cost of having one captured node in the WSN (4a) and Q_{avg} the average cost of having one captured node in the WSN (4b). Table II also shows optimal proportional gain μ, Kalman gain K_f and the static feedforward signal u_{ff} for each of the four cases, where we choose $R = R_{log}$ and $Q = Q_{max}$.

Table III shows the optimal control parameters: proportional gain μ, static feedforward signal u_{ff} and Kalman gain K_f for network setup IV.

By comparing Figures 3 and 4, we observe that network performance under a node capture attack highly depends on the type of costs Q and R we choose. Table III shows that if the controller is designed with costs Q_{max} and R_{log}, the magnitude of the proportional gain μ is 30 times bigger than the magnitude of the gain μ designed using cost Q_{avg} and R_{lin}. Such a behavior nicely reflects the LQ optimal control method. The optimization criteria is the cost of the control action J. Since it is inexpensive to have compromised nodes in the network and it is quite expensive to revoke them, the proposed control action is to let all the compromised nodes stay in the network. Therefore, we can conclude that the LQR and LQG controllers should be designed using maximum unit cost of having compromised nodes in the network Q_{max}, which represents the upper bound on the impact one compromised node $c_k \in \mathcal{C}$ has on the network.

From Figure 4 (costs Q_{max} and R_{log}), we observe that the LQR controller is performing faster than the LQG controller. This is because the LQG controller contains the state estimator, which highly depends on the initial state of estimation. In these simulations, the initial estimation state is set to $\hat{x}_0 = 0$. Such an initial estimation state was chosen for two reasons: to examine how fast and accurate the estimator in fact is and to show that the LQG controller is able to maintain the network connectivity even when the estimation process starts from an arbitrary estimation state.

[5]Such a characterization requires spatial statistical analysis and was not provided in this paper due to the space limitations.

TABLE II

COMPUTATION OF COSTS (Q_{max}, Q_{avg}, R_{lin}, R_{log}) AND CONTROL PARAMETERS (M , μ, u_{ff}, K_f) AS FUNCTIONS OF NETWORK PARAMETERS (N, P, K)

Parameters	**Setup I**	**Setup II**	**Setup III**	**Setup IV**
N	10^3	10^3	10^4	10^4
P	10^4	10^4	10^5	10^5
K	50	100	100	200
R_{lin}	62500	10^6	10^6	$16 \cdot 10^6$
R_{log}	6475.7	53019	53019	358980
Q_{max}	974.61	62237	62488	$3.99 \cdot 10^6$
Q_{avg}	30.22	20283	459.74	$3.93 \cdot 10^5$
M	199	100	999	500
u_{ff}	-8.67	-4.77	-47.69	-24.63
μ	0.34	1.04	1.04	3.29
K_f	0.9512	0.9512	0.9512	0.9512

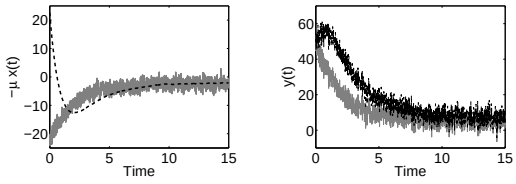
TABLE III

COMPUTATION OF CONTROL PARAMETERS (μ, u_{ff}, K_f) FOR ($N = 10^4$, $P = 10^5$, $K = 200$) AND COST PAIRS (Q, R) FOR SETUP IV, TABLE II

Fig.	2	3	4	5
R	R_{lin}	R_{lin}	R_{log}	R_{log}
Q	Q_{max}	Q_{avg}	Q_{max}	Q_{avg}
μ	0.45	0.11	3.29	0.99
K_f	0.9512	0.9512	0.9512	0.9512
u_{ff}	-22.51	-17.40	-24.63	-23.81

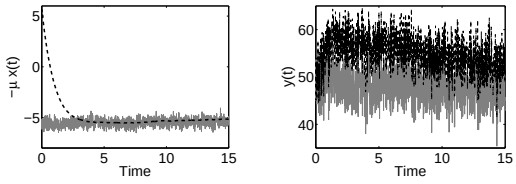
VI. CONCLUSION

In this paper we studied the physical node capture attack problem in wireless sensor networks. Currently, there is no adversarial model for this problem [3] in the area of wireless



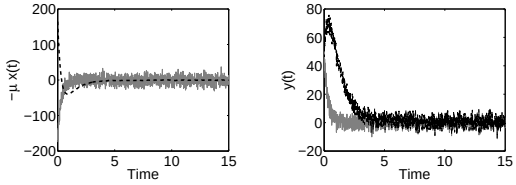
(a) (b)

Fig. 2. Comparison in network response using LQR and LQG controller: (a) Control signal $-\mu x(t)$ - number of nodes to be removed, (b) Output signal $y(t)$ - number of nodes with all keys compromised, (Network setup: N = 10000, x_0 = 50, λ = 0.05, $\omega_n = \omega_\alpha = \mathcal{N}(0, 10)$, $Q = Q_{max}$, $R = R_{lin}$)



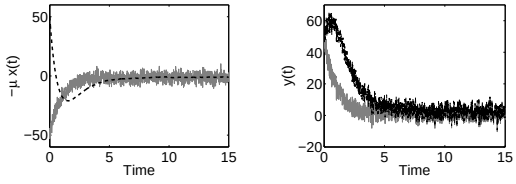
(a) (b)

Fig. 3. Comparison in network response using LQR and LQG controller: (a) Control signal $-\mu x(t)$ - number of nodes to be removed, (b) Output signal $y(t)$ - number of nodes with all keys compromised, (Network setup: N = 10000, x_0 = 50, λ = 0.05, $\omega_n = \omega_\alpha = \mathcal{N}(0, 10)$, $Q = Q_{avg}$, $R = R_{lin}$)



(a) (b)

Fig. 4. Comparison in network response using LQR and LQG controller: (a) Control signal $-\mu x(t)$ - number of nodes to be removed, (b) Output signal $y(t)$ - number of nodes with all keys compromised, (Network setup: N = 10000, x_0 = 50, λ = 0.05, $\omega_n = \omega_\alpha = \mathcal{N}(0, 10)$, $Q = Q_{max}$, $R = R_{log}$)



(a) (b)

Fig. 5. Comparison in network response using LQR and LQG controller: (a) Control signal $-\mu x(t)$ - number of nodes to be removed, (b) Output signal $y(t)$ - number of nodes with all keys compromised, (Network setup: N = 10000, x_0 = 50, λ = 0.05, $\omega_n = \omega_\alpha = \mathcal{N}(0, 10)$, $Q = Q_{avg}$, $R = R_{log}$)

security, thus preventing any comprehensive approach to model and mitigate the physical node capture attack.

In this work, we showed that the physical node capture attack can be studied using a control theory framework, that simultaneously incorporates physical node capture, detection of cloned nodes and revocation of compromised nodes, followed by key refreshment of the valid nodes.

Using control theory methods, we showed that the network response to node capture attacks can be characterized using a proportional controller. We developed two network response strategies based on optimal control theory and showed the optimization problem can be formulated explicitly in terms of the network as well as logical key graph parameters. Using optimal control theory, we obtained the minimal revocation rate as a control parameter, which guarantees secure network connectivity and hence stability under the attack. We provided extensive simulation results to verify the proposed network response strategies.

The practical implications of our work are: it enables (a) analysis of the network's stability and resilience against the physical node capture attack, (b) characterization of adversarial behavior and strategies and (c) computation of the optimal revocation rates, in terms of network parameters and cryptographic quantities, to maintain secure network connectivity in the presence of the attack.

APPENDIX
DERIVATION OF THE COSTS Q AND R

Consider a WSN with N nodes, where each node $n_i \in \mathcal{N}$ is assigned the set of K keys from the key pool of $P \gg K$ keys, according to the random key management scheme proposed in [4]. Let β_i denote the number of nodes sharing a given key $k_i \in \mathcal{K}_t$. When a subset of $\mathcal{K}_{t,i} \subset \mathcal{K}_t$ is randomly selected for a node $n_i \in \mathcal{N}$, one particular key is selected with probability $\frac{K}{P}$. This selection can be modeled as a Bernoulli random variable and the probability distribution $\mathcal{P}(\beta)$ can be modeled as the binomial distribution $\mathcal{B}(N, \frac{K}{P})$ [7], $\mathcal{P}(\beta) = \binom{N}{\beta}\left(\frac{K}{P}\right)^{\beta}\left(1-\frac{K}{P}\right)^{N-\beta}$.

A. Derivation of the Cost Q

Consider the situation of one compromised node c_k holding K keys. Node c_k shares each key k_i with β_i other nodes in the network. Since an adversary is assumed to actively listen on all of the exposed links, i.e., the links he holds the keys for, the communication on all such links is considered to be broken. Therefore, the unit cost Q reflects the impact of one captured node c_k on network connectivity.

Theorem 4: The worst case cost of having one compromised node in the network is equal to $Q_{max} = \binom{N}{2}\frac{K^3}{P^2}$.

Proof: The maximum number of links exposed to an adversary by capturing one node $c_k \in \mathcal{C}$ is equal to $\sum_{i\in\mathcal{K}_{t,c_k}}\binom{\beta_i}{2}$. The expected value of the maximum number of links exposed to an adversary can be calculated as:

$$\mathbb{E}\left[\sum_{i\in\mathcal{K}_{t,c_k}}\binom{\beta_i}{2}\right] = \sum_{i\in\mathcal{K}_{t,c_k}}\mathbb{E}\left[\frac{\beta_i^2-\beta_i}{2}\right] \quad (19a)$$

$$= \frac{K}{2}\left(\mathbb{E}[\beta_i^2] - \mathbb{E}[\beta_i]\right) \quad (19b)$$

$$= K\left(\frac{K^2}{P^2}\right)\frac{N(N-1)}{2} = \binom{N}{2}\frac{K^3}{P^2} \quad (19c)$$

By noting that each node $n_j \in \mathcal{N}$ holds exactly K keys, equation (19a) can be expressed as (19b), which can be written as (19c) due to the fact that β_i is a binomial random variable. Thus (19c) represents the worst case cost Q_{max}. ■

Theorem 5: The average cost of having one compromised node in the wireless sensor network equals the expression

TABLE IV
ADDITIONAL NOTATION USED FOR APPENDIX

Symbol	Definition
$\mathcal{K}_{t,j\cup l}$	Union of keys held by nodes n_j and n_l
β_i	Number of nodes sharing the key k_i
Z	Avg. number of links node $c_k \in \mathcal{C}$ shares with other nodes
C_0	Cost of sending one key to one user
p	Probability that any two nodes in the WSN share a link

$Q_{avg} = \binom{N}{2} p \left\{ 1 - \left[1 - \left(\frac{K}{P}\right) \frac{N\left(\frac{K}{P}\right)-1}{N-1} \right]^K \right\}$, where p represents the probability that any two nodes in the WSN share a link.

Proof: Consider a WSN represented as a random graph $G(\mathcal{N}, \mathcal{K}_t)$ where a set of vertices $\mathcal{N}$ represents sensor nodes deployed in a WSN and a set of edges $\mathcal{K}_t$ represents secure communication links at time t. The average number of links node $c_k \in \mathcal{C}$ shares with other nodes in a WSN can be expressed as:

$$Z = \sum_{(j,l)\in(\mathcal{N}\times\mathcal{N})} \mathbb{1}\{(j,l) \in \mathcal{K}_t \text{ and } K_{t,j\cap l} \cap K_{t,c_k} \neq \emptyset\} \quad (20)$$

where $\mathbb{1}\{(j,l) \in \mathcal{K}_t$ and $K_{t,j\cap l} \cap K_{t,c_k} \neq \emptyset\}$ represents the indicator function. The expected value of the average number of links node c_k shares with other nodes is given as:

$$\mathbb{E}[Z] = \sum_{(j,l)\in(\mathcal{N}\times\mathcal{N})} \mathbb{P}[\{(j,l) \in \mathcal{K}_t \text{ and } K_{t,j\cap l} \cap K_{t,c_k} \neq \emptyset\}] \quad (21)$$

By the assumption that node deployment is independent of key assignment, expression (21), can be written as:

$$\mathbb{E}[Z] = \sum_{(j,l)\in(\mathcal{N}\times\mathcal{N})} \mathbb{P}[K_{t,j\cap l} \cap K_{t,c_k} \neq \emptyset]\mathbb{P}[(j,l) \in \mathcal{K}_t] \quad (22)$$

Assuming that existences of each link $(j,l) \in \mathcal{K}_t$ are independent, identically distributed (i.i.d.) random variables, equation (22) can be represented as:

$$\mathbb{E}[Z] = \binom{N}{2} p(1 - \mathbb{P}[(K_{t,j\cap l}) \cap K_{t,c_k} = \emptyset]) \quad (23)$$

As in [7], the probability $\mathbb{P}_1 = \mathbb{P}[K_{t,j\cap l} \cap K_{t,c_k} = \emptyset]$:

$$\begin{aligned} \mathbb{P}_1 &= \sum_{i=1}^{K} (|(K_{t,j\cap l})| = i, (K_{t,j\cap l}) \cap K_{t,ck} = \emptyset) \\ &= 1 - \left(\frac{K}{P}\right) \frac{N\left(\frac{K}{P}\right)-1}{N-1} \end{aligned} \quad (24)$$

Therefore, equation (23) can now be written as:

$$\mathbb{E}[Z] = \binom{N}{2} p \left\{ 1 - \left[1 - \left(\frac{K}{P}\right) \frac{N\left(\frac{K}{P}\right)-1}{N-1} \right]^K \right\} \quad (25)$$

■

For simulation purposes, Q_{max} and Q_{avg} are normalized:

$$\begin{aligned} Q_{max} &= \frac{N\cdot(N-1)}{40}\frac{K^3}{P^2} \\ Q_{avg} &= \frac{N\cdot(N-1)}{40} p \left\{ 1 - \left[1 - \left(\frac{K}{P}\right) \frac{N\left(\frac{K}{P}\right)-1}{N-1} \right]^K \right\} \end{aligned}$$

B. Derivation of the Cost R

Node revocation takes place when there are nodes in the revocation list. A compromised node gets revoked by broadcasting the revoked list of keys, held by the compromised nodes, to all the valid nodes in a WSN. In order to maintain connectivity, the revocation action is followed by the key refreshment action, during which all the nodes with revoked keys are being refreshed with new, freshly generated keys. Therefore the unit cost of revoking compromised nodes mainly reflects the communication cost. Many key refreshment methods are possible. In this paper we focus only on two: linear-update and tree-structure-update method.

Theorem 6: The unit revocation cost R, using a linear-update method is equal to $R_{lin} = C_0 \frac{K^2 N}{P}$, where C_0 denotes the cost of sending one key.

Proof: Consider the situation of one compromised node $c_k \in \mathcal{C}$ in the WSN. There are β_i nodes sharing each of the compromised keys $k_i \in \mathcal{K}_{t,c_k}$, held by the captured node c_k. Since β_i is a binomial random variable, the expected number of nodes holding each key $k_i \in \mathcal{K}_{t,c_k}$ is equal to $\mathbb{E}[\beta] = N\frac{K}{P}$. In order to refresh K keys held by the captured node c_k using a linear-update method, each key k_i is sent to $N\frac{K}{P}$ nodes that share the key with the captured node, where the cost of sending one key to one user is defined as C_0. Therefore, the cost of revoking one node c_k using linear-update method is equal to $C_0 \frac{K^2 N}{P}$. ■

Theorem 7: The unit revocation cost R, using tree-structure-update method [8] is equal to $R_{log} = KC_0 \log \frac{KN}{P}$.

Proof: Consider the situation where the WSN has a hierarchical structure, i.e., there exists a root node in the WSN and every other node has a parent node. In such a structure freshly generated key k_i is not send to each of $N\frac{K}{P}$ nodes sharing the key, but only to child nodes of the captured key c_k. Therefore, each key k_i is sent to $\log N\frac{K}{P}$ nodes and the revocation cost is equal to $R_{log} = KC_0 \log \frac{KN}{P}$. ■

For simulation purposes, R_{lin} and R_{log} are normalized $R_{lin} = \frac{K^2 N}{P}$; $R_{log} = K \log \frac{KN}{P}$.

REFERENCES

[1] H. Chan and A. Perrig, "Security and privacy in sensor networks," *IEEE Computer Magazine*, pp. 103–105, 2003.

[2] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Broadcast control channel jamming: Resilience and identification of traitors," in *IEEE International Symposium on Information Theory, ISIT 2007*, June 2007, pp. 2496 –2500.

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

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[5] P. Dorato, C. T. Abdullah, and V. Cerone, *Linear Quadratic Control, An Introduction*. Malabar, FL: Krieger Publishing Company, 2000.

[6] T. Bonaci, L. Bushnell, and R. Poovendran, "Probabilistic analysis of covering and compromise in a node capture attack," Network Security Lab (NSL), Seattle, WA, Techical Report #001, 2010.

[7] P. Tague and R. Poovendran, "A canonical seed assignment model for key predistribution in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 3, no. 4, 2007.

[8] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 60–96, 2004.