Game-Theoretic Defense Strategies for Mitigating Gray Hole Attacks on Energy-Limited Sensors in Wireless Sensor Networks

Ines Carole Kombou Sihomnou *†, Abderrahim Benslimane†, Ahmed H. Anwar Hemida‡, Gabriel Deugoue*, and Charles Kamhoua‡
*Universty of Dschang, Dschang, Cameroon
†Avignon University, Vaucluse, France
‡DEVCOM Army Laboratory, Maryland, USA
Email: ines-carole.kombou-sihomnou@alumni.univ-avignon.fr, abderrahim.benslimane@univ-avignon.fr, a.h.anwar@knights.ucf.edu, agdeugoue@yahoo.fr, charles.a.kamhoua.civ@army.mil

***Abstract*—Wireless Sensor Networks (WSNs) have improved efficiency and accuracy in various applications, including military and healthcare. However, gray hole attacks are damaging and difficult-to-detect attack that causes communication delays, packet loss, and significant energy losses. The paper aims to limit the energy effect of gray-hole attacks in WSNs by presenting the interaction between an attacker and their target as an extensive game with incomplete information. Equilibrium profiles, once computed and achieved, guarantee optimal protection for the defender and maximum damage potential for the attacker. The simulation showed that the model can force the attacker to behave normally in a WSN, limiting energy consumption.**

***Index Terms*—Bayesian Game, Black Hole Attack, DoS, Extensive Form Game, Flooding Attack, Gray Hole Attack, WSN.**

I. Introduction

WSNs are distributed systems that consist of a data collection point (BS or sink) and a network of sensor nodes. Wireless sensor networks are used for a variety of purposes, including monitoring and recording physical conditions (wind, speed, and pressure) [1], and many more. The captured data is sent to the collection point within a WSN via multi-hop routing. Data routing from the source to the collecting point is inextricably linked to trust at intermediate nodes [2]. Multi-hop communication is vulnerable to a variety of attacks, including flood, vampire, black hole, and gray hole attacks [3]. These kinds of attacks have a serious influence on the energy consumption of sensor nodes. Cryptography methods have proven to be useful in some circumstances against this kind of attack. However, because sensor nodes are typically powered by batteries, the energy cost of security approaches might be prohibitively high and must thus be kept to a minimum.

In a black hole attack, the malicious node utilizes its routing protocol to make itself known to the cluster nodes. Following that, independent of routing table verification, it is promoted as having the shortest route to the target node [4]. Once the path is established, it is up to the malicious node to either remove all packets traveling through it or allow a fraction of packets to flow through while dropping the rest: the gray hole attack. The gray hole attack is comparable to the black hole attack in many ways. The gray hole node, unlike the black hole node, does not instantly block all packets that travel through it; instead, some packets are passed to actual nodes, making them even more challenging to identify. Consider the flood-based routing protocol attack, in which the requester always obtains the answer from the malicious node first. As a result, a faked route is constructed, and the aggressive node can decide, for example, to transmit User Data Protocol (UDP) packets while blocking Transmission Control Protocol (TCP) packets. This article focuses on sensor node energetic defense against gray hole attacks.

Network nodes in a WSN may not always possess complete knowledge of the network's nodes. A malicious node, however, often has extensive knowledge about the routing protocol employed in the network and the identities of the nodes it seeks to target. Based on this information, the malicious node may opt to execute an attack that not only disrupts or halts communication but also depletes the energy levels of the affected nodes. To defend against these attacks, we utilize game theory to determine and evaluate action profiles that lead to optimal Nash equilibrium solutions.

The goal of this study is to provide a defense strategy that would reduce the energy effect of gray hole attacks on the sensor nodes. Our key contributions are:

- An application of incomplete information game model between the sender and the attacker against gray hole attack;
- A mathematical model that demonstrates the application of the game and enables optimal defensive strategies to

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

be formulated against the attacker.

The rest of the paper is described as follows: section II provides an overview of related work in this area. Section III outlines the novelty that our work brings and the Bayesian equilibrium analysis of the presented game. Section V presents the results of the simulations, and section VI concludes the work.

II. Literature Review

Denial of Service (DoS) attacks, including gray hole attacks (GHAs), have been studied by various authors against WSNs and MANETs (Mobile Ad Hoc Networks) [5]. Pal et al. [6] present a technique for detecting packet drop attacks in a network, with a focus on synchrophasor data packets. The suggested approach categorizes packet loss as being caused by congestion or an attacker. To identify and categorize packet drop attacks, they employ a classification method based on packet latencies and patterns. This approach is useful in TCP for sending data that requires changes in switches. However, the process of performing TCP handshakes and subsequent validation requires additional computational and communication resources. These added operations could potentially consume more energy, especially in high-traffic scenarios, leading to increased power consumption in the network infrastructure. Ila et al. [7] have also outlined a technique for protecting mobile ad hoc networks (MANETs) against blackhole and grayhole attacks. The suggested methodology deploys the Ad-hoc On-demand Distance Vector (AODV) protocol for route discovery, the Artificial Bee Colony Algorithm (ABC) for route refining and identification of malicious nodes, and the Artificial Neural Network (ANN) for classification of normal and malicious nodes. Simulation results demonstrate improvements in packet delivery rate, throughput, and delay over existing methods. However, implementing the stated security mechanism consumes more energy within the nodes.

Sensors are employed in vehicular networks, which are also vulnerable to various types of attacks, such as GHAs which compromise security and deplete energy resources. In defense, Elham et al. [8] propose a routing technique based on Q-Learning (QL-TRT). The approach consists of choosing the best neighbor based on a Markov decision process. Q-Learning is used to know the trust value of links and select the most reliable route. The performance of QL-TRT is demonstrated in the detection of GHA attacks. The computational and communication power to implement these techniques can be high. Consequently, it would be important to weigh the advantages of security against the disadvantages in terms of energy consumption.

In recent years, game theory has proven to be a useful mathematical tool for describing the interactions of two or more supposed rational and intelligent individuals. Vijayalaskmi et al. [9] propose a host abuse detection system that uses game-theoretic approaches to identify malicious nodes and improve security. The system uses reactive and proactive methods,

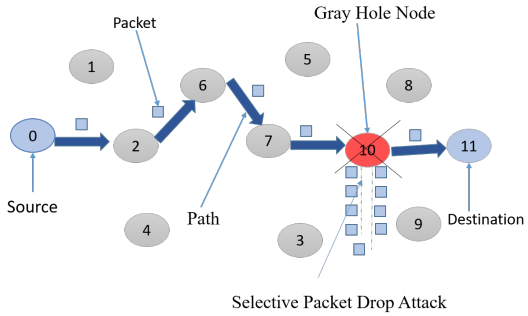

Fig. 1: Gray hole attack

observing node behavior and increasing the transfer counter with each transmitted packet. However, this requires constant monitoring and energy consumption. The suggested approach requires a significant amount of energy, which may cause the sensor batteries to be depleted prematurely.

Doshi et al. [10] model the gray hole attack as an extensive two-player game. The suggested solution's implementation techniques rely on feedback control algorithms AIAD (additive-increase multiple-decrease), MIMD (multiple-increase multiple-decrease), and MIAD (multiple-increase additive-decrease). However, this technique is limited by the simplifying assumptions made by the authors, specifically that all participants are aware of the increment and decrement patterns of the algorithms used by the packet sender. These methods are typically used to manage TCP congestion and are unsuitable for sensor networks with limited energy resources. The battery life of the sensors can rapidly deteriorate due to frequent broadcasts and attempts to adjust bandwidth.

While the literature mentioned above has enhanced the defense and detection rates of GHA, it has also led to increased energy consumption attributed to extended computation times, operations, models, and other parameters. Our approach is geared towards identifying an optimal strategy that factors in the cost associated with identifying a new route for packet transmission in case the initially proposed route is not utilized, all without incurring additional energy usage. The primary goal of this research is to develop an effective defense against GHA to save sensor energy within a WSN.

III. Defense Model Based on Bayesian Game

In this paper, the problem addressed is described in Fig. 1. We have three main actors: the source node (Normal node) of the packets, the gray hole node, and the destination node of the packets. The source sends packets to the target, which must travel through the malicious node's route. When packets reach the malicious node, they might be routed to the target, destroyed, or routed to an unknown node. Because even a normal node might remove packets due to congestion, the source node cannot discover that the gray node is an attacker.

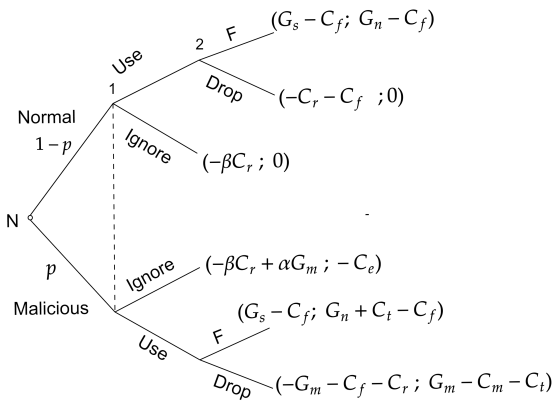

Fig. 2: Extensive form of the game.

As a result, we must create a game that accounts for all of these factors.

A. Game model

The interaction between the sender node (player 1) and the gray hole node or attacker (player 2) is modeled as a non-cooperative game in extensive form with incomplete information, as described in Fig. 2. The gray hole node is either malicious or normal. Thus, it can either forward packets (denoted by *F*) or not forward them (denoted by *Drop*) and its type θ_2^i is unknown to the sender. $\theta_2^i \in \Theta$, where Θ represents the set of player types.

$$\theta_2^i = \begin{cases} \text{Malicious} & \text{if } i = 1 \\ \text{Normal} & \text{if } i = 0 \end{cases}$$

$$\theta_1 = \quad \text{Normal}$$

The game starts when the sender chooses to communicate through the path set up by the gray hole node. We assume that nature determines the gray hole node's maliciousness with a probability $(p, 1-p)$. We interpret nature here as the chance that a randomly chosen node is a gray hole.

Let forward (*F*) and Drop be two possible actions for the attacker; therefore, the space of possible actions is $A_2 = \{F, Drop\}$. The sender has the option to utilize (*Use*) or decline (*Ignore*) the attacker's established route, resulting in a possible action space of $A_1 = \{Use, Ignore\}$. The last parameter of the game is utility; we have $U = \{u_1, u_2\}$ where $u_i : A \times \Theta \mapsto \mathbb{R}$ is the utility function of the player i. The players are considered to be rational; therefore, they will always seek to maximize their payoffs in the game. The attacker's goal is to do the sender as much damage as possible; the primary resource targeted is energy.

We introduce G_m and C_m, which respectively represent the gain and cost for a malicious node when it performs an attack on the network. In a WSN, G_m can be observed as the energy consumed by the transmitter as a result of the attack. A node may behave maliciously without dropping packets to disguise its malicious identity. When a node (malicious or regular) shows normal behavior (forwarding the packets it receives), it obtains a gain. Let G_n and C_f represent the gain of acting normally (forwarding the packets) and the cost of forwarding the packets, respectively. G_n can be defined as the trust acquired from the network nodes, the benefit of participating (being named) in the election of a cluster head, or even participation in the routing protocol. The sender earns a G_s gain from the destination node if the malicious node receives and sends the packets to the destination. As a result, the sender's payoff is $G_s - C_f$, and the malicious node's payoff is $G_n + C_t - C_f$. If, on the other hand, the node intercepts and deletes the packets, the sender loses the gains that represent the value of the package; therefore, his payoff is equivalent to $-G_m - C_f - C_r$ and the payoff of the malicious node is $G_m - C_m - C_t$. Where C_r is the cost of the sender node looking for a new route to send the packets. If the sender decides to send its packets along the same route, $C_r = 0$. When a malicious node forwards packets, it obtains C_t in addition to its gain. C_t records the history of malicious actions; for example, if a node has deleted a packet maliciously, it risks detection in the future, and C_t represents this risk. When a node drops packets, its chances of being selected for the next route discovery are diminished.

We assume that $G_m > G_n$; otherwise, the attacker has no motive to attack. When a sender decides not to use the shortest route a node declares, it looks for an alternative route. If the node claiming the shortest path is m a normal node, its reward is 0 because it is not utilized and the payoff of the sender's node is $-\beta C_r$. However, if this node is malicious, it will lose C_e, which reflects the cost of being vulnerable to discovery. Therefore the reward of the sender is $-\beta C_r + \alpha G_m$, where α and β represent respectively the trust and false alarm rates with $\alpha, \beta \in [0, 1]$. To prevent a normal node that has turned malicious from carrying out ignored attacks, we presume that normality is not a stable reality over time.

TABLE I: Symbol description

Symbol	Signification
G_s	The sender's gain for a successfully transmitted packet
G_n	The gain of the node after performing a normal activity
G_m	Gain of a node after performing a malicious activity
C_t	The cost of risk for the next round of the game
C_r	The Cost of searching for a new route
C_m	The Cost of performing a malicious activity
C_f	The cost of forwarding a packet from one node to another
C_e	The cost of exposure
β	False alarm rate
α	True positive rate

(a) For the malicious type of the node

	UseUse	UseIgnore	IgnoreUse	IgnoreIgnore
F	$G_n + C_t - C_f$,$G_s - C_f$	$G_n + C_t - C_f$,$G_s - C_f$	$-C_e$; $-\beta C_r + \alpha G_m$	$-C_e$; $-\beta C_r + \alpha G_m$
Drop	$G_m - C_m - C_t$; $-G_m - C_f - C_r$	$G_m - C_m - C_t$; $-G_m - C_f - C_r$	$-C_e$; $-\beta C_r + \alpha G_m$	$-C_e$; $-\beta C_r + \alpha G_m$

(b) For the normal type of node

	UseUse	UseIgnore	IgnoreUse	IgnoreIgnore
F	$G_n - C_f$, $G_s - C_f$	$G_n - C_f$, $G_s - C_f$	0; $-\beta C_r$	0; $-\beta C_r$
Drop	$G_m - C_m - C_t$; $-G_m - C_f - C_r$	$G_m - C_m - C_t$; $-G_m - C_f - C_r$	$-C_e$; $-\beta C_r + \alpha G_m$	$-C_e$; $-\beta C_r + \alpha G_m$

TABLE II: Expected utility value matrix for normal form game

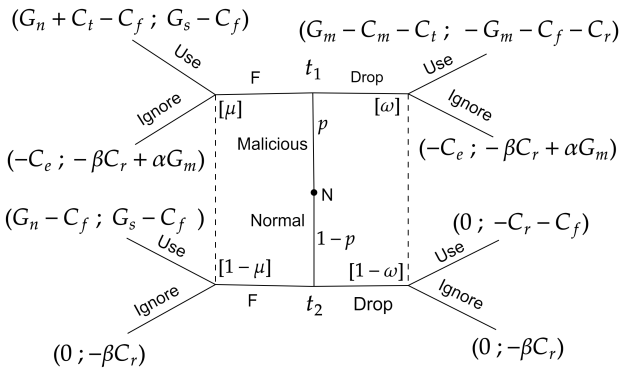

Fig. 3: Extensive form of the Bayesian game.

B. Evaluation of equilibrium

The extensive form of the game as described in Fig. 2 is useful for intuitive explanations, however, this structure is not suitable for analytical purposes, unlike the normal form of the game. Nevertheless, the game illustrated in Fig. 2 does not lend itself readily to normal representation. To achieve this goal, we transform the extensive form game into a Bayesian game to extract the Bayesian normal form (a game-theoretic concept that extends the traditional notion of normal-form games to incorporate uncertainty or players' beliefs about the actions of other players) for evaluation. Fig. 3 represents the extensive form of the Bayesian game. μ and $\omega \in [0,1]$ denote the sender's belief about his information set based on the attacker's strategies, and $t_1, t_2 \in \Theta$. Using the normal form of the Bayesian games specified in Table II, we can compute the strategy profiles of the players who can verify the Bayesian Nash equilibrium. It should be noted that converting an extended game with imperfect knowledge into a Bayesian game may lead to ambiguity in defining equilibrium. Therefore, we translate all discovered profile equilibrium formally to clarify the meaning.

IV. Perfect Bayesian Nash equilibrium analysis

In the following, we analyze for sets of strategy profiles $(S_2^m, S_2^n, S_1^1 S_1^2, \mu; \omega)$ that lead to PBNE where:

1) S_2^m denotes the malicious type strategy of the attacker;
2) S_2^n denotes the normal type strategy of the attacker;
3) $S_1^1 S_1^2$ is the strategy combination for the sender, where S_1^1 represents its response to the malicious attacker's strategy S_2^m and S_1^2 represents its response to the normal attacker's strategy S_2^n.

Perfect Bayesian Nash Equilibrium (PBNE) strategies and beliefs satisfy the following conditions [11].

1) *Sequential rationality*: The player's strategies must be sequentially optimal given their beliefs: each strategy must be optimal in expectation given the beliefs.
2) *Beliefs*: The player with the move must have a belief about which node in the info set has been reached by the game's play at each info set.
3) *On-the-equilibrium Path*: Baye's rule and the player's equilibrium strategies must be used to determine belief in the information set on the equilibrium path.
4) *Off-the-equlibrium path*: Whenever possible, the beliefs at any off the equilibrium-path information set must be determined from the strategy profile using the Bayes Rule.

Condition 2 is trivial, and can be seen in Fig. 3. According to condition 1, we have the evaluation of dominant strategies described as follows:

- Given the information of μ

$$u_1(Use, \mu) = \mu(G_s - C_f) + (1-\mu)(G_s - C_f) = G_s - C_f \tag{1a}$$

$$\begin{aligned} u_1(Ignore, \mu) &= (-\beta C_r + \alpha G_m)\mu - (1-\mu)(\beta C_r) \\ &= \alpha \mu G_m - \beta C_r \end{aligned} \tag{1b}$$

$u_1(Use, \mu) > u_1(Ignore, \mu) \implies \mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}$
If $\mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}$, the dominant strategy is *Use* otherwise, the dominating strategy is *Ignore*.

- Given the information described by ω

$$\begin{aligned} u_1(Use, \omega) &= \omega(-G_m - C_f - C_r) + (1-\omega)(-C_r - C_f) \\ &= -\omega G_m - (C_r + Cf) \end{aligned} \tag{2a}$$

$$u_1(Ignore,\omega) = (-\beta C_r + \alpha G_m)\omega - (1-\omega)(\beta C_r) = \alpha\omega G_m - \beta C_r \quad (2b)$$

$u_1(Use,\omega) > u_1(Ignore,\omega) \implies \omega < \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}$ (always false). The dominant strategy of the sender is *Ignore*.

Now, what are the dominant strategies of the attacker for the actions of the sender?

- For the malicious type of the attacker, when $\mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}$ and $\omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}$ we have:

$$u_2(F) = G_n + C_t - C_f \quad (3a)$$

$$u_2(Drop) = -C_e \quad (3b)$$

$u_2(F) > u_2(Drop) \implies G_n + C_t - C_f > -C_e$. As $G_n + C_t - C_f > -C_e$ the dominant strategy for the attacker is *F*.
For $\mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}$ and $\omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}$ we have:

$$u_2(F) = u_2(Drop) = -C_e \quad (4a)$$

The malicious player is indifferent to his strategies; he can play *Drop* or *F*.

- For the normal type of the attacker, if $\mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}$ and $\omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}$ we have:

$$u_2(F) = G_n - C_f \quad (5a)$$

$$u_2(Drop) = 0 \quad (5b)$$

The best response for the regular type of attacker is *F*.
if $\mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}$ and $\omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}$ we have:

$$u_2(F) = u_2(Drop) = 0 \quad (6)$$

According to the above computations, the equilibrium strategies profile are:

1) $(F, F, \textit{UseIgnore}, \mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$, which translates into, depending on the restrictions on μ and ω, if the normal node chooses to Use or Ignore the route given by an attacker to deliver its packets to the destination, forwarding (F) the packets is always the best strategy for an attacker. Each profile has its own expected utility for players, so we have:

$$EU(attacker) = p(G_n + C_t - C_f) + (1-p)0 = p(G_n + C_t - C_f) \quad (7)$$

$$EU(sender) = p(G_s - C_f) - (1-p)\beta C_r = p(G_s - C_f + \beta C_r) - \beta C_r \quad (8)$$

2) $(Drop, F, \textit{IgnoreIgnore}, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$, which translate to depending on μ and ω constraints, the best response for a normal node will always be the Ignore the issued route, regardless of the type of attacker. The expected utilities of the players for this profile are:

$$EU(attacker) = -pC_e + (1-p)0 = -pC_e \quad (9)$$

$$EU(sender) = p(-\beta C_r + \alpha G_m) - (1-p)\beta C_r = p\alpha G_m - \beta C_r \quad (10)$$

3) $(Drop, Drop, \textit{IgnoreIgnore}, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$

Equilibrium profiles 2 and 3 are equivalent in terms of the gains expected by players.

A. Pooling equilibrium

By conditions 3 and 4 of the PBNE, we seek to determine the exact values of μ and ω. When dealing with pooling strategies, i.e. when $S_1^m = S_1^n$, the values of μ and ω are calculated as follows.

- For the Strategy profile $(Drop, Drop, \textit{IgnoreIgnore}, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$ we have:

$$\omega = \frac{P_m(Drop) \times p}{P_n(Drop) \times (1-p) + P_m(Drop) \times p} = p \quad (11)$$

We cannot establish the exact value of μ since it is off the equilibrium path; this leads to the conclusion that there are an infinite number of pooling solutions for the value of μ according to the following structure: $(Drop, Drop, \textit{IgnoreIgnore}, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega = p > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$.

- For the strategy profile $((F, F, \textit{UseIgnore}, \mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}), G_m < G_n + 2C_t + C_m - C_f)$

$$\mu = \frac{P_m(F) \times p}{P_n(F) \times (1-p) + P_m(F) \times p} = p \quad (12)$$

Similarly, we cannot determine the exact value of ω. The structure of this equilibrium profile is as follows: $((F, F, \textit{UseIgnore}, \mu = p < \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m}), G_m < G_n + 2C_t + C_m - C_f)$

B. Seperating equilibrium

For separative equilibrium strategies, i.e. when $S_1^m \neq S_1^n$, ω and μ are on the path to equilibrium, which makes it possible to determine the exact values of μ and ω.

$$\omega = \frac{P_m(Drop) \times p}{(1-p)P_n(drop) + P_m(Drop) \times p} = 1 \quad (13)$$

$$\mu = \frac{P_m(F) \times p}{(1-p)P_n(F) + P_m(F) \times p} = 0 \quad (14)$$

We have the following separating equilibrium: $(Drop, F, \textit{IgnoreIgnore}, \mu = 0 > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega = 1 > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$

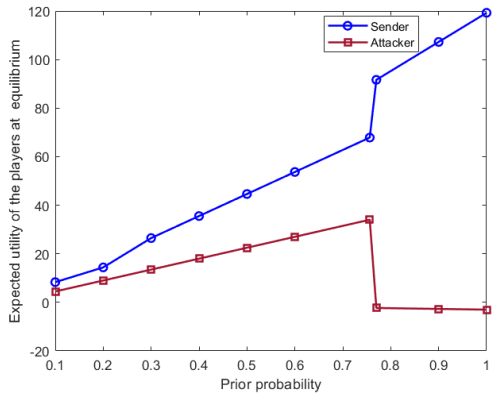

Fig. 4: The utility of players at equilibrium as a function of prior probability p for the strategy profiles

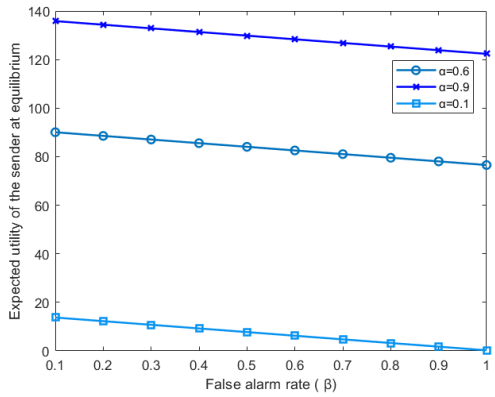

Fig. 5: The utility of normal node at equilibrium as a function of false alarm rate β for the strategy profiles

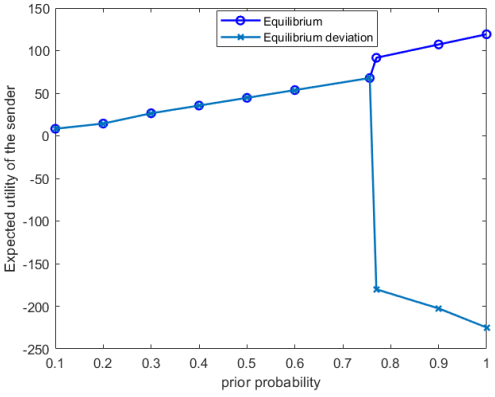

Fig. 6: Comparison of the sender's expected utility: strategies at the Nash equilibrium and deviation from it

V. Simulations and Results

We analyze our model and compute the Bayesian perfect Nash equilibrium between a sensor node and the CH in this section. The PBNE has the best CH action profiles against grayhole attacks. We established the following game parameters: $G_m = 200$, $G_n = 15$, $G_s = 100$, $C_t = 5$, $C_m = 20$, $\beta = 0.05$, $\alpha = 0.6$, $C_r = 15$, $p = 0.5$, $C_f = 10$. Let's first recall that $\mu = p$ for pooling strategy profiles according to the calculations performed in the previous section. We set $G_m > G_n$ to show the advantage a node has in attacking. The distance between the values of G_n and G_m is made to highlight the robustness of the model; increasing the value of G_n can only improve the results obtained.

Fig. 4 shows the variation of the players' expected utility function (reward) at equilibrium described in eqs. (7) to (10) as a function of a prior probability. At equilibrium, for $\mu < \frac{G_s - C_f + \beta C_r}{\alpha G_m}$, i.e., when the sender decides to send packets via the route received from the attacker and the attacker decides to forward them, we see that the expected utility of both the attacker and the sender of the packets increases. However, when $\mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}$, i.e., the attacker sends an attack route and the sender decides not to use it. We observe that the attacker's utility decreases because he exposes himself to free detection since the sender doesn't choose his route. The drop point of the attacker's utility in Fig. 4 can be attributed to the node normal's shift in the assessment regarding the attacker beyond $\mu = \frac{G_s - C_f + \beta C_r}{\alpha G_m}$. The equilibrium profiles for the attacker are relevant either when the attacker is forwarding packets normally (the lower right portion of the figure) or when the attacker is engaged in an attack (the upper left portion of the figure). In the latter scenario, the sender disregards the route provided by the attacker, resulting in reduced payoffs for the attacker. Given the assumption of the attacker's rationality, the goal is to maximize gains, which is consistent with the first case. Therefore, based on Fig. 4, the model forces the attacker to act in a normal, non-attacking manner.

Recall that one of our goals is to mitigate the attack's adverse effects on the target or sending node. To accomplish this, we move the target node away from the equilibrium location indicated by the equilibrium action profile $(Drop, Drop, IgnoreIgnore, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$. According to the two types of attackers, we assume that the target moves unilaterally, adopting the action profile $((Drop, Drop, UseUse, \mu > \frac{G_s - C_f + \beta C_r}{\alpha G_m}, \omega > \frac{(\beta-1)C_r - C_f}{(\alpha+1)G_m})$ while maintaining the equilibrium conditions. The losses incurred by the transmitter as a result of its deviation from the calculated equilibrium profile (3) are shown in Fig. 6 of the document.

In the following, we set the value of $p = 0.77 > \frac{G_s - C_f + \beta C_r}{\alpha G_m}$. Fig. 5 shows the impact of the false alarm rate on the utility of the normal node. When the false alarm rate increases, the efficiency of the normal node decreases. However, the usefulness of a normal node improves significantly with the detection rate. For a detection rate of 60%, the suggested model is impacted by only 14.92% for a maximum false alarm rate ($\beta = 1$), which reduces as the detection rate increases.

VI. Conclusion

This study focuses on modeling and analyzing a gray-hole attack that disrupts communication and reduces sensor node battery life. The attack is modeled using game theory, and optimal strategies are determined across various scenarios. The interaction between packet sender nodes and gray hole nodes is characterized as a Bayesian game, with both participants exhibiting rational and intelligent behavior. The study explores scenarios conducive to Perfect Bayesian Nash Equilibrium (PBNE), where the sender has the discretion to decide whether to utilize the route transmitted by a node. The outcomes are transferable to MANET and WANET networks, with no additional energy burdens. Future research may consider involuntary packet deletion for congested nodes and a dynamic version of the current game.

Acknowledgment

Research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-21-1-0326. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein. Work by Ines Carole Kombou Sihomnou was partially supported by the Schlumberger Foundation Faculty for the Future program.

References

[1] Dionisis Kandris, Christos Nakas, Dimitrios Vomvas, and Grigorios Koulouras. Applications of wireless sensor networks: an up-to-date survey. *Applied System Innovation*, 3(1):14, 2020.

[2] Na Fan and Chase Q Wu. On trust models for communication security in vehicular ad-hoc networks. *Ad Hoc Networks*, 90:101740, 2019.

[3] Mohammad Nafis Ul Islam, Ahmed Fahmin, Md Shohrab Hossain, and Mohammed Atiquzzaman. Denial-of-service attacks on wireless sensor network and defense techniques. *Wireless Personal Communications*, 116:1993–2021, 2021.

[4] Ahmad Hasan, Muazzam A Khan, Balawal Shabir, Arslan Munir, Asad Waqar Malik, Zahid Anwar, and Jawad Ahmad. Forensic analysis of blackhole attack in wireless sensor networks/internet of things. *Applied Sciences*, 12(22):11442, 2022.

[5] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, 21(2):210, 2019.

[6] Seemita Pal, Biplab Sikdar, and Joe Chow. Real-time detection of packet drop attacks on synchrophasor data. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 896–901. IEEE, 2014.

[7] Pooja Rani, Sahil Verma, Gia Nhu Nguyen, et al. Mitigation of black hole and gray hole attack using swarm-inspired algorithm with artificial neural network. *IEEE Access*, 8:121755–121764, 2020.

[8] Elham Mohammadzadeh Mianji, Gabriel-Miro Muntean, and Irina Tal. Trustworthy routing in vanet: A q-learning approach to protect against black hole and gray hole attacks. In *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pages 1–6, 2023.

[9] S Vijayalakshmi, S Bose, G Logeswari, and T Anitha. Hybrid defense mechanism against malicious packet dropping attack for manet using game theory. *Cyber Security and Applications*, 1:100011, 2023.

[10] Chintan Ketankumar Doshi, Sreecharan Sankaranarayanan, Vidyashankar B Lakshman, and K Chandrasekaran. Game theoretic modeling of gray hole attacks in wireless ad hoc networks. In *Proceedings of the International Conference on Signal, Networks, Computing, and Systems: ICSNCS 2016, Volume 1*, pages 217–226. Springer, 2017.

[11] Joel Watson. A general, practicable definition of perfect bayesian equilibrium. *unpublished draft*, 2017.