GAME THEORY BASED DECEPTION
FOR SECURITY IN NETWORKS

By
RENUKA KANDREGULA

Bachelor of Engineering in Computer Science
Anna University
Chennai, India
2006

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2010
GAME THEORY BASED DECEPTION
FOR SECURITY IN NETWORKS

Thesis Approved:

Dr. Johnson P Thomas
Thesis Adviser

Dr. Subhash Kak

Dr. V. Sarangan

Dr. A. Gordon Emslie
Dean of the Graduate College
ACKNOWLEDGMENTS

Firstly, I would like to thank my adviser Dr. Johnson P Thomas for his support, advice, time and patience. He showed me different ways to approach a research problem and taught me that persistence is essential to accomplish any goal.

I, furthermore, would like to thank my committee members Dr. Subhash Kak and Dr. V. Sarangan for their valuable suggestions, time and effort in helping me complete my thesis.

I would like to extend my sincere gratitude to my family for their unconditional support and encouragement to pursue my interests.

I would also like to thank my best friend Mr. Siddarth Kotha who stood beside me through all the good and bad times and who has been a constant source of moral support and strength.

Last but not the least, I would like to thank my good friends who helped me stay focused on my graduate study and helped me complete this work.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Section 1.1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Section 1.2 Problems in Existing Models</td>
<td>2</td>
</tr>
<tr>
<td>Section 1.3 Proposed Work</td>
<td>3</td>
</tr>
<tr>
<td>Section 1.4 Document Outline</td>
<td>4</td>
</tr>
<tr>
<td>II. REVIEW OF LITERATURE</td>
<td>5</td>
</tr>
<tr>
<td>Section 2.1 Literature Review</td>
<td>5</td>
</tr>
<tr>
<td>III. METHODOLOGY</td>
<td>8</td>
</tr>
<tr>
<td>Section 3.1 Problem Definition</td>
<td>8</td>
</tr>
<tr>
<td>Section 3.2 Proposed Solution</td>
<td>8</td>
</tr>
<tr>
<td>Section 3.3 Proposed Game Model</td>
<td>9</td>
</tr>
<tr>
<td>Section 3.4 Proposed Game Structure</td>
<td>9</td>
</tr>
<tr>
<td>Section 3.5 Dynamic Game Approach</td>
<td>10</td>
</tr>
<tr>
<td>Section 3.6 Players of the Game</td>
<td>11</td>
</tr>
<tr>
<td>Section 3.7 Strategies of the Players</td>
<td>12</td>
</tr>
<tr>
<td>Section 3.8 Outcome of the Game</td>
<td>12</td>
</tr>
<tr>
<td>Section 3.9 Strategy Spaces for the Players</td>
<td>13</td>
</tr>
<tr>
<td>Section 3.10 Profit and Cost Function for the Attacker</td>
<td>14</td>
</tr>
<tr>
<td>Section 3.11 Utility and Cost Function for the Defender</td>
<td>15</td>
</tr>
<tr>
<td>Section 3.12 Payoff Matrix for the Players</td>
<td>17</td>
</tr>
<tr>
<td>Section 3.13 Payoff Matrix Analysis</td>
<td>18</td>
</tr>
<tr>
<td>Section 3.14 Parameter and Information Analysis</td>
<td>20</td>
</tr>
<tr>
<td>Section 3.15 Analysis of Profit for the Attacker</td>
<td>21</td>
</tr>
<tr>
<td>Section 3.16 Analysis of Utility for the Defender</td>
<td>27</td>
</tr>
</tbody>
</table>
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Payoff Matrix to the Players</td>
<td>17</td>
</tr>
<tr>
<td>4.1 Payoff Matrix to the Players with Numerical Estimates</td>
<td>34</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Proposed Game Model</td>
<td>10</td>
</tr>
<tr>
<td>3.2 Fuzzy Logic Systems</td>
<td>21</td>
</tr>
<tr>
<td>3.3 Fuzzification of Input ‘Criticality’</td>
<td>23</td>
</tr>
<tr>
<td>3.4 Fuzzification of Input ‘Damage’</td>
<td>24</td>
</tr>
<tr>
<td>3.5 Aggregation of Outputs Criticality and Damage</td>
<td>26</td>
</tr>
<tr>
<td>3.6 Fuzzification of Input ‘Threat’</td>
<td>28</td>
</tr>
<tr>
<td>3.7 Aggregation of Outputs Criticality and Threat</td>
<td>28</td>
</tr>
<tr>
<td>4.8 Sample Game Play</td>
<td>36</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

1.1 Introduction

Sensor Networks have great potential in different fields such as industrial and military applications, battlefield operations and also regular commercial applications. Sensor Networks involve deploying a large number of small nodes over flexible network architectures. The sensor nodes in the network are equipped with wireless transmitters and receivers to perform distributed tasks. These sensors have limited memory power and battery life. Since the nodes run on battery, power and energy consumption becomes a constraint. Resource constraints limit the security mechanisms that can be implemented in sensor networks. Hence it is relatively easy to launch an attack on sensor networks. Although a lot of work has been done on protecting sensor networks using key management techniques, little work has been reported on responding to these attacks. Responses include shutting down the network (or a part of it), strengthening the protection mechanisms of the network, trying to bypass the attacker and deceiving the attacker.
In this thesis, we propose deception as an appropriate response mechanism. Although deception is not applicable in all scenarios, it is useful in a number of cases. For example, deception allows most of the network to function as normal. Deception allows the defending network to manipulate the behavior of the attacker. It also wastes the resources of the attacker.

To apply deception, we need a reactive kind of architecture – one that reacts by deceiving when it is suspicious that someone is attacking. We propose Game Theory as the basis of a deception framework. Existing systems can be modeled as games which are then used to study the properties of the systems. Game theory when applied to address the security issue in sensor networks is a modeling technique which can be used to anticipate and explain the actions of all the agents involved in competitive situations and can be used to test and determine the relative optimality of different strategies. As a result, aspects of game theory are being applied to war games and global military strategies. We apply game theory to model a deception game in Sensor Networks.

1.2 Problems in Existing Models

Due to resource scarcity, protecting sensor networks is difficult using the traditional approaches. Due to the resource critical characteristics and high probability of failures, it is very difficult to implement complex security algorithms. Conventional security models like Key management schemes for confidentiality, integrity and authentication are resource intensive. Such techniques cause a huge amount of communication and computing overhead. [1] Basar presented a game theoretic model to
detect intrusions, and the interactions between the attacker node and the defending node are modeled. In their model, a third fictitious player is added to the game and a cost function is modeled to minimize the incurred costs by both the attacker and defender. The addition of a third player induces complexity. A two-player game has also been proposed by Agah et al [2] [3] to address the security mechanism between the attacker and defender and the optimal strategy depends only on the payoff function. This assumption has limitations in a real network. Only the payoff function might not be sufficient to address the optimal strategy as there will be other network parameters that have to be taken into account like the risk associated, the cost of effort associated with the attacker and the defender and also the network utility parameters such as the resource constraints, etc. They have proposed a game theoretic model to model the interactions between the service provider and the attacker. The object of the attacker is to find a path between two nodes namely the source and destination and thereby determine the intrusions using sampling techniques. In our case, the objective of the attacker is not to find a path between two nodes, rather it is to launch an attack on a node in the network and the defender node can either detect the attack, deceive the attacker or the attack can go undetected and the attacker will gain access to the information in the network and may disrupt the network.

1.3 Proposed work

In the game of deception, we formulate an attacker-defender model. The proposed model allows the defender to keep defending the attacker using deception techniques to keep the network secure. A new approach using deception is suggested for the defender which acts as a defense mechanism. The role of the deception is to provide
false information to the attacker and hence can be employed as a defense technique in order to conceal what the attacker is looking for. A game theoretic model represents the game between an attacker and defender. Estimation factors and fuzzy logic theory are used to estimate the payoff functions and the strategies for both the attacker and the defender.

1.4 Document Outline

The rest of the document is organized as follows. Chapter 2 presents the literature review and background which addresses the problems of existing models in detail. Chapter 3 presents the problem definition, proposed solution, the game model in detail including the parameter definitions, payoff functions, game formulation and the game analysis. Chapter 4 presents the implementation details, sample game play and the equilibrium. Chapter 5 presents the conclusion of the work followed by references.
CHAPTER II

REVIEW OF LITERATURE

2.1 Literature Review

Many security mechanisms have been proposed to address the problem of security in Sensor Networks. The most widely used security mechanisms have many drawbacks and limitations. The encryption techniques such as Wired Equivalent Privacy otherwise known as WEP used in Sensor Networks have been shown to be easily breakable and easily hacked [4]. New and more secure techniques of encryption can be easily breakable when not configured properly [5]. So, security is the top priority in a Sensor Network.

Encryption hardware techniques such as Network Cards would be an expensive alternative and more bulky in nature.

A lot of research work has been made to address the security issues in sensor networks. Many security techniques that focus on encryption as a security mechanism focus mainly on the level of security that they provide but do not address the problem of complexity that they pose. The complexity can be defined as the usage of large numbers and loops of manipulating data. The other security mechanism is the key establishment technique in cryptography. Disclosing a key with each packet requires too much energy [6]. They provide better security mechanisms but they also have a drawback which is again a large
calculation intricacy and also a large performance hit since the keys incur bottlenecks in terms of storage [7]. Also, the key management technique requires an engineered solution that makes it unsuitable for sensor network application. This will make the Sensor Network susceptible to attacks. The other security mechanism is the usage of routing protocols. But research studies show that they have proved to be inefficient in the way that they incorporate a problem of communication between the nodes.

Mechanisms such as Intrusion Detection prove to be quite effective but they incur a large number of resource allocation overheads and hence best results cannot be achieved due to the network resource constraints. Also a lot of research has been conducted on anomaly detection against insider attacks [8], where the objective is to detect a deviation from a pre-determined model of normal system behavior. However this is difficult since experimental studies from many generic approaches show that these approaches have a very high false rate.

Also, different security protocols are available for sensor networks. The SNEP protocol [9] has low communication overhead providing baseline security primitives like data confidentiality, data authentication and reply protection. The TESLA protocol [10] uses a symmetric key mechanism. A wide range of attack detection mechanisms have been developed to access and analyze the risk in organizations and financial markets [11]. In wireless sensor networks, it is hard to estimate security level accurately because of the complexity of the factors involved. To generate one way key-chain, the sender chooses the last key randomly and generates the remaining values by successively applying one way function. The protocol discloses the key once per time interval and restricts the
number of authenticated senders. The LEAP protocol is based on observation that no single security requirement accurately suits all types of communication in a wireless network. There are four different keys to whom the sensor node is communicating with. Basar and Oldser [12] describe a mechanism for establishing a key between two sensor nodes that is based on the common trust of a third node somewhere within the network. Security can be achieved by identifying the possibility of attacks and the extent of damage caused by the attack.

A number of approaches have been identified to defend against attacks. Karlof and Wagner [13] defend against attacks by identifying the compromised part of the network effectively routing around the unavailable portion.
CHAPTER III

METHODOLOGY

3.1 Problem Definition

Sensor networks have limited memory, computational power and energy or battery life. Therefore it is difficult to implement complex key management schemes. We propose a reactive architecture which reacts when there is suspicious of an attack on it. It reacts by defending the attacker using deception. This is achieved by using Game Theory. We design a deception game model to effectively secure the network against attacks. The payoffs of the defender and attacker are derived using utility parameters and game theory. This proposed game model is novel as it introduces deception as a security response mechanism unlike existing works. Furthermore, fuzzy logic is used to obtain a numerical estimate for parameters like criticality, threat, damage and cost associated with the game model.

3.2 Proposed Solution

The deception based framework shown in this thesis uses a game theoretic decision making system. The game is played between the attacker and the defender. The model uses utility parameters and game theory concepts to derive a
payoff relation. The players (Attacker and the Defender) payoffs are a function of the profit or loss to the players and also the cost incurred. The defender chooses an appropriate response that will maximize the payoff of the defender by minimizing the attacker’s payoff. The deception is integrated into the game. Based on the objective of the defender, the payoff is defined, and therefore the strategy that gives the maximum payoff is chosen by the defender. Although some work has been done on using game theory for securing sensor networks, using game theory for deception is an unexplored area.

3.3 Proposed Game Model

We define a model using game theory for securing sensor networks. We define a non cooperative dynamic game between an attacker and a defender in the network and analyze the strategies. We study the game leading to the deception strategy for the defender. We model our game for the attacker and the defender to maximize their payoffs. The attacker tries to maximize his payoff by trying to be successful in his attacks and the defender tries to maximize his payoff by deceiving the attacker so as to minimize the risk. The gain for the attacker is based on the payoff value and the cost spent on attacking a node. The gain for the defender will be based on the payoff value and the cost incurred due to deception.

3.4 Proposed Game Structure

There are two types of players - A Defender ‘D’ and an Attacker ‘A’. We consider the interactions between the attacker and defender as a repeated dynamic game. Our basic idea is for the defender to detect the attack and deceive the attacker in a way
that it reduces the payoff to the attacker and hence the network can be effectively secured against attacks. The figure below shows a model of our proposed game.

![Figure 3.1 Proposed Game Model](image)

### 3.5 Dynamic Game Approach:

We consider dynamic games of incomplete information i.e some players take actions before others and these actions are observed to some extent by some other players. We consider the game-theoretic modeling of security in sensor networks. We consider the interactions between the defender and attacker as a repeated game. We assume the following. In this paper, we investigate the application of deception by the defender against attackers. To make this game a simple game of incomplete information, we endow the attacker with some private information which we describe as the type of
the attacker. The defender has no type associated with it. To successfully deceive the attacker, the defender faces the following two critical challenges.

- Firstly, the defender does not have perfect knowledge about the outcome of its interactions with the attackers.

- Second we consider the attacker’s type to be intelligent and regular. Intelligent attackers are the ‘smart’ ones who adapt their attacking strategies based on some belief or knowledge about the defense mechanism employed by the defender so as to avoid being detected and consequently being deceived. Another type of attackers are the regular ones who randomly choose to attack or not to attack.

To address the above two challenges, in this paper, we consider the real world scenario where the defender can only observe the outcome of the detected attacks but has no knowledge about undetected attacks.

3.6 Players of the Game

There are two types of players - A Defender ‘D’ and an Attacker ‘A’. As mentioned earlier, the attackers are classified into two types: Intelligent and Regular. Intelligent attackers make optimal attacking decisions based on their knowledge of the defensive mechanism. Regular attackers on the other hand blindly launch attacks or choose not to attack at all. Our thesis work limits to the consideration of only regular attackers.
3.7 Strategies

Defender - The defensive strategy employed by the defender is to deceive the attacker if an attack is detected and observed. Let us define the trade-off parameter $\gamma \in [0,1]$. We normalize $\gamma$ such that the probability of deceiving the attacker is $1 - \gamma$. So when $\gamma = 0$, all attacks are defended by employing deception and when $\gamma = 1$, no attack is defended.

Attacker - The attacker’s strategy determines whether to launch an attack or not to attack. An attacker may choose to attack or not to attack.

3.8 Outcome of the Game:

The strategy combination of the defender and the attacker determines the outcome of the game. In this game, we consider the following four possible outcomes:

- An attack is launched and is not detected by the defender - no deception strategy is implemented since the defender has no knowledge about undetected attacks.
- An attack is launched and is detected by the defender - deception strategy is implemented.
- The attacker chooses not to attack and the defender does nothing - no deception strategy is implemented.
- The attacker chooses not to attack and the defender thinks that there is an attack and implements deception which we can term it as a needless deception.

In practice, other possibilities may exist. For example, the defender might detect an attack but misidentify the type of the attack or target of the attack. For the purpose of the
paper, we assume that the defender makes a Boolean decision of whether an attack has been launched or not.

Therefore there are only four possible outcomes:

- {Attack, No Deception}
- {Attack, Deception}
- {No Attack, No Deception}
- {No Attack, Deception}

As mentioned earlier, the defender can observe only the second outcome i.e {Attack, Deception}. An attacker on the other hand may be able to observe all the outcomes based on the previous interactions with the defender. The attacker will be able to update its beliefs about the outcomes of the game as the game proceeds.

3.9 Strategy Spaces for the Attacker and Defender

In game theory, a player's strategy in a game is a complete plan of action for whatever situation might arise; this fully determines the player's behavior. A player's strategy will determine the action the player will take at any stage of the game, for every possible history of play up to that stage. A strategy space (sometimes called a strategy combination) is a set of strategies for each player which fully specifies all actions in a game available to all the players in a game. Each player considers all the other players and their possible strategies, and then chooses a specific strategy from his strategy set. All players make a choice, the choices are revealed and the game ends with each player receiving some payoff. Each player’s choice may influence the final outcome for all the
players. For our game model, we define the following four strategies for the attacker and defender.

\[ S_{\text{nd}} \rightarrow \text{No Deception} \]
\[ S_{\text{d}} \rightarrow \text{Deception} \]
\[ S_{\text{a}} \rightarrow \text{Attack} \]
\[ S_{\text{na}} \rightarrow \text{No Attack} \]

The strategy space for the defender is denoted as: \( S_D = \{S_d, S_{\text{nd}}\} \).

The strategy space for the attacker is denoted as: \( S_A = \{S_a, S_{\text{na}}\} \).

### 3.10 Utility, Cost and Payoff Function for the Attacker

An intelligent attacker chooses to launch an attack that is successful or not to launch an attack based on some previous beliefs. On the other hand, the regular attacker randomly chooses to attack or not to attack. The objective of an intelligent attacker is to maximize his payoff and choose the strategy that maximizes his payoff.

For the attacker, two parameters are considered – Net Profit and Cost. The attacker not only considers the profit \( P \) from a successful attack but also considers cost and potential risks of the action \( C_A \).

**Cost Function of the Attacker:**

The cost function of the attacker \( C_A = c_1 + c_2 \) has two components:

*Initial Cost:*

An intelligent attacker would research and study the network and try to find a way to launch a successful attack. On the other hand, a regular attacker will
randomly launch an attack. The initial cost is the cost incurred by any type of attacker for launching an attack. It is denoted by $c_1$.

*Conditional Cost:*

Costs related to potential risks of an attacker to be detected and deceived are described by this component. In detail, if the defender detects the attack and employs deception to deceive the attacker, the attacker incurs another cost called as the conditional cost denoted by $c_2$. If the defender does not detect the attack, it means that the attacker will not incur this cost component.

**The net profit or payoff (P) to the attacker:**

The profit $P$ can be expressed as a weighted information parameter. In particular, the profit can be expressed in terms of the type of information the attacker is gaining access to as a result of launching an attack and also the damage that the attacker is causing to the network as a result of the attack. The profit $P$ can be quantified to a numerical value using Fuzzy Logic Theory. The net profit is a difference between the Profit and the Cost Components.

$$P = P - (c_1 + c_2)$$

We will show how the profit can be modeled in terms of information in the following section.

**3.11 Cost and Payoff Function for the Defender**

The defender has two main objectives:

i) To detect as many attacks as possible and hence deceive the attacker.

ii) To reduce the number of needless deceptions.
Loss to the defender due to needless deceptions:

Let \( L_{\text{ND}} (i) \) be the loss of the defender associated with needless deceptions. Needless Deceptions are those deceptions employed by the defender when there is no attack by the attacker but the defender thinks that there is an attack and employs deception. We can define \( L_{\text{ND}} (i) \in [0,1] \) and is the loss associated with needless deceptions in one time slot. ‘i’ can be 0 or 1; that is 0 when there is no attack and 1 when there is an attack. Hence we get:

\[
L_{\text{ND}} (0) = 1 \quad \text{and} \quad L_{\text{ND}} (1) = 0
\]

Cost Function for the Defender:

The cost of implementing deception is the price a defender must pay to deceive the attacker in case of a detected attack. It is denoted by \( C_D \). The cost of deception depends on how much effort is spent to deceive the attacker. Typical cost of defense estimate can be obtained by using the fuzzy logic theory and is shown in the following section.

Payoff Utility Function for the Defender:

For simplicity, we define the payoff utility function for the defender \( U_D (t) \) at time ‘\( t \)’ as a linear combination with respect to a network. The payoff function is defined as a function of the utility parameters: criticality of information, the defender is deceiving or not deceiving (weight) and number of nodes the defending node is connected to which can be termed as the threat to the network. Threat is the potential harm that the attacker can cause to the network as a result of the attack.

\[
U_D (t) = f[W_D (t), N_D (t)]
\]
$W_D$ is the weight of the information the defending node is carrying (Criticality) and $N_D$ is the number of nodes the defending node is connected to and it is also the number of nodes the attacker is destroying or gaining access to which is nothing but the threat to the network.

The utility function to the defender can also be estimated using Fuzzy Logic Theory.

### 3.12 Payoff Matrix for the Attacker and Defender:

The matrix is denoted by $M$ and has matrix elements $M_{11}, M_{12}, M_{21}, M_{22}$.

<table>
<thead>
<tr>
<th>Defender</th>
<th>Detected and Deceive</th>
<th>Undetected/No Deception</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack</td>
<td>$P - (C_1 + C_2), U - C_D$</td>
<td>$P - C_1, 0$</td>
</tr>
<tr>
<td>No Attack</td>
<td>$0, L_{ND}$</td>
<td>$0, 0$</td>
</tr>
</tbody>
</table>

**Table 3.1 Payoff Matrix to the Players**
3.13 Payoff Matrix Analysis

The payoff matrix is denoted by M. The elements $M_{11}, M_{12}, M_{13}, M_{14}$ represent the payoffs to the attacker and defender under the strategy {Attack, Deceive}, {Attack, No Deception}, {No Attack, Deceive}, {No Attack, No Deception} respectively.

- $M_{11}$ represents the payoffs to the attacker and defender under the strategy set: {Attack, Deceive}.
- $M_{12}$ represents the payoffs to the attacker and defender under the strategy set: {Attack, No Deception}.
- $M_{21}$ represents the payoffs to the attacker and defender under the strategy set: {No Attack, Deceive}.
- $M_{22}$ represents the payoffs to the attacker and defender under the strategy set: {No attack, No Deception}.

Payoff Analysis under the Strategy {Attack, Deceive}:

Under the strategy {Attack, Deceive}, $M_{11}$’s value is: $P - (C_1 + C_2), U - C_D$.

When the attacker attacks and the defender detects the attack and employs deception, the net payoff to the attacker would be a difference of values between the profit ‘P’ and the sum of cost components ‘$C_1+C_2$’. The cost components $C_1$ and $C_2$ are both considered for the attacker here because $C_1$ represents the initial cost incurred by the attacker and $C_2$ represents the conditional cost due to the result of being attacked and deceived by the defender. The defender’s payoff would be a difference of values between the payoff utility function for the defender ‘U’ and the cost of defense ‘$C_D$’.
Payoff Analysis under the Strategy \{Attack, No Deception\}:

Under the strategy \{Attack, No Deception\}, the value of $M_{12}$ is $P - C_1$, 0. The attacker’s payoff would be a difference of values between profit ‘$P$’ and only the initial cost component ‘$C_1$’. Here, we don’t consider the cost component ‘$C_2$’ for the attacker because when we say there is no deception, it means that the defender has not been able to detect the attack and hence, the attacker incurs no additional conditional cost component of being deceived. On the other hand, the payoff to the defender is zero since there is no deception involved. The defender has not been able to detect the attack and hence does not employ any deception mechanism to defend the attack.

Payoff Analysis under the Strategy \{No Attack, Deceive\}:

Under the strategy \{No attack, Deception\}, the payoff to the attacker is zero since the attacker chooses not to attack and there is no cost component or profit incurred to the attacker. The payoff to the defender is in terms of loss due to needless deceptions denoted by ‘$L_{ND}$’ because the defender incurs a loss of needless deception even when there is no attack.

Payoff Analysis under the Strategy \{No Attack, No Deception\}:

Under the strategy \{No attack, No deception\}, the payoff to the attacker is zero since the attacker chooses not to attack and there is no cost component or profit incurred to the attacker. The payoff to the defender is also zero because there is no deception involved. The defender does not employ any deception mechanism since there is no attack detected.
3.14 Parameter and Information Analysis: 

**Quantifying the profit ‘P’ of the attacker:**

Profit to the attacker can be determined with respect to the criticality of the information the attacker is gaining as a result of the attack and also the damage that the attacker is causing to the sensor network. We consider the damage and criticality with respect to the sensor network. If the attacker gains critical information and causing a high damage, we can determine the profit. But the relationship between criticality and damage has gray areas in which it is difficult to identify a threshold value above which the profit to the attacker is low or high. In order to accurately address this issue, we use Fuzzy Logic and Fuzzy Sets to calculate the profit.

**Using Fuzzy Logic**

Fuzzy Logic is determined as a set of mathematical principles for knowledge representation based on degrees of membership rather than on crisp membership of classical binary logic. Fuzzy Logic uses a continuum of logical values between 0 (completely false) and 1 (completely true). Classical binary logic can be considered a special case of multi-valued fuzzy logic. Crisp set theory is governed by a logic that uses one of only two values true or false. This logic cannot represent vague concepts and therefore fails to give the answers on paradoxes and areas where estimation over a wide set of values is needed. The basic idea of fuzzy set theory is that an element belongs to a fuzzy set within a certain degree of membership. The figure below depicts a fuzzy logic system.
3.15 Analysis of the Attacker’s Profit:

Let $X$ (criticality of information), $Y$ (Damage) and $Z$ (Profit) be three linguistic variables. $A_1$, $A_2$ and $A_3$ (high, moderate, low) are linguistic values determined by fuzzy sets on the universe of discourse $X$ (How critical is the information that the attacker is attacking); $B_1$, $B_2$ and $B_3$ (Catastrophic, Moderate, Negligible) are linguistic values determined by fuzzy sets on the universe of discourse $Y$ (The damage caused to the network); $C_1$, $C_2$ and $C_3$ (High, Medium, Low) are linguistic values determined by fuzzy sets on the universe of discourse $Z$ (Profit gained by the attacker).

We define the rules that govern the fuzzy logic:
Rule 1:
IF  X is A1    IF Criticality is High
AND Y is B1    AND Damage is Catastrophic
THEN Z is C1    THEN Profit is High

Rule 2:
IF  X is A2    IF Criticality is Moderate
OR Y is B2    OR Damage is Moderate
THEN Z is C2    THEN Profit is Moderate

Rule 3:
IF  X is A3    IF Criticality is Low
AND Y is B3    AND Damage is Negligible
THEN Z is C3    THEN Profit is Low

Note that the given rules are not comprehensive. Rules for X (A1, A2, A3) and Y(B1, B2, B3) can be given in all possible combinations of linguistic values which we can derive more sets. For example, a valid rule can be when X is A2 and Y is B1 (The Criticality is Moderate but Damage is Catastrophic), then C can be set to C1, C2 or C3 (high, medium, low) depending on the requirement of the user. The rules given here are for illustration.

We use Mandani Style fuzzy inference to estimate the profit gained by the attacker.

Step 1: Fuzzification

The first step is to get the crisp inputs required. Let ‘r’ be the actual criticality of information and ‘s’ be the actual damage caused to the network. We determine the degree to which these inputs approximate to each of the fuzzy set.

In fuzzy theory, the fuzzy set A of universe X is defined by function \( \mu_A(x) \) called the membership function of set A.

\[
\mu_A(x) = 1 \text{ if } x \text{ is totally in } A
\]
\[
\mu_A(x) = 0 \text{ if } x \text{ is not in } A
\]
$0 < \mu_A(x) < 1 \text{ if } x \text{ is partially in } A$

For any element $x$ of universe $X$, membership function $\mu_A(x)$ equals the degree to which $x$ is an element of set $A$. This degree, a value between 0 and 1, represents the degree of membership, also called the membership value, of element $x$ in set $A$.

Thus by combining each fuzzy set for $X$, $Y$ and $Z$, we get:

**Criticality** $X = [\mu_{x=A_1}, \mu_{x=A_2}, \mu_{x=A_3}]$

**Damage** $Y = [\mu_{y=B_1}, \mu_{y=B_2}, \mu_{y=B_3}]$

**Profit** $Z = [\mu_{z=C_1}, \mu_{z=C_2}, \mu_{z=C_3}]$

Thus from the crisp values (actual values), we can plot the membership value or the fuzzified inputs which represent the degree to which each input belongs to the fuzzy set, within the corresponding universe of discourse.

**Fuzzification of Input: Criticality ‘r’**

![Figure 3.3 Fuzzification of Input ‘Criticality’](image)

23
Fuzzification of Input: Damage ‘s’

Figure 3.4 Fuzzification of Input ‘Damage’

Let \( r_1, r_2, r_3 \) and \( s_1, s_2, s_3 \) be the corresponding membership values resulting from fuzzification of crisp inputs \( r \) and \( s \), in the fuzzy sets \( X \) and \( Y \) respectively.

Step 2: Rule Evaluation

The second step is to take the fuzzified inputs

\[
\mu_{X=A_1} = r_1, \quad \mu_{X=A_2} = r_2, \quad \mu_{X=A_3} = r_3 \quad \text{and} \quad \mu_{Y=B_1} = s_1, \quad \mu_{Y=B_2} = s_2, \quad \mu_{Y=B_3} = s_3
\]

And apply them to the antecedents of the fuzzy rules. If a given fuzzy rule has multiple antecedents, the fuzzy operator (AND, OR) is used to obtain a single number that represents the result of antecedent evaluation.
OR OPERATION: \( \mu_{A \cup B} (x) = \max [\mu_A (x), \mu_B (x), \ldots] \)

AND OPERATION: \( \mu_{A \cap B} (x) = \min [\mu_A (x), \mu_B (x), \ldots] \)

Let \( t_1, t_2, t_3 \) be the result of fuzzy logic operators for the fuzzy set \( Z \). Thus we get:

**Rule 1:**
IF X is A1 (r1) AND Y is B1 (s1) THEN Z is C1 (t1)
\[ \mu_{c1} (Z) = \min [\mu_{a1} (X), \mu_{b1} (Y)] = t1 \]

**Rule 2:**
IF X is A2 (r2) OR Y is B2 (s2) THEN Z is C2 (t2)
\[ \mu_{c2} (Z) = \max [\mu_{a2} (X), \mu_{b2} (Y)] = t2 \]

**Rule 3:**
IF X is A3 (r3) AND Y is B3 (s3) THEN Z is C3 (t3)
\[ \mu_{c3} (Z) = \min [\mu_{a3} (X), \mu_{b3} (Y)] = t3 \]

**Step 3: Aggregation of the Rule outputs:**

Aggregation of the outputs is a process of unification of the outputs of all rules. In other words, we take the membership functions of all rule consequents previously obtained and combine them into a single fuzzy set. The resultant area represents all the membership values for the profit estimate.
The figure above depicts the aggregation process. In the figure, t1, t2 and t3 indicate the aggregate membership value for each of the rules. The x-axis values indicate the range in the universe of discourse $Z$ corresponding to membership values t1, t3 and t3.

**Step 4: Defuzzification:**

The final step is to obtain a numerical estimate for the profit of the attacker. The fuzziness helps us to evaluate the rules but the final output of a fuzzy system has to be a crisp number. We use the centroid technique to find the final estimate. We find the value, referred as center of gravity (COG), indicates the point where a vertical line would slice the aggregate set into two equal masses. It can be expressed as:

$$COG = \frac{\int_{a}^{b} \mu_A(x) \, x}{\int_{a}^{b} \mu_A(x)}$$
In theory, COG is calculated over a continuum of points in the aggregate output membership function but in practice, a reasonable estimate can be obtained by calculating it over a sample of points.

Thus we get:

$$COG = \frac{(K_1 + K_2 + \ldots + K_i) t1 + (K_i + \ldots + K_j) t2 + (K_j + \ldots + K_n) t3}{(i\ast t1) + ((n+i-j)\ast t2) + ((n-i-j)\ast t3)} \Rightarrow P\ (Profit)$$

From the calculation shown above, we can get the final profit estimation of the attacker to be $P$ and the net profit would be $P - C_A$ as mentioned in the payoff matrix.

### 3.16 Analysis of the Defender’s Payoff Utility:

The calculation of the defender’s utility payoff is similar to that of the calculation of Profit estimate to the attacker. We use Fuzzy logic and Fuzzy sets to get an estimate of the defender’s payoff utility. The four steps of fuzzy logic are implemented namely Fuzzification, Rule Evaluation, Aggregation and Defuzzification. The parameters used for calculating the defender’s payoffs are Criticality, Threat and Utility. The rule base for the defender’s utility and the fuzzification of input ‘Threat’ are described below.

**Rule 1:**

IF X is A1

OR Y is B1

THEN Z is C1

IF Criticality is High

OR Threat is Extreme

THEN Utility is High

**Rule 2:**

IF X is A2

OR Y is B2

THEN Z is C2

IF Criticality is Moderate

OR Threat is Moderate

THEN Utility is Moderate

**Rule 3:**

IF X is A3

OR Y is B3

THEN Z is C3

IF Criticality is Low

OR Threat is Low

THEN Utility is Low
Fuzzification of input: Threat ‘s’:

Figure 3.6 Fuzzification of Input ‘Threat’

Aggregation of the Rule outputs:

Figure 3.7 Aggregation of Outputs
CHAPTER IV

IMPLEMENTATION

4.1 Implementation

In this chapter, a case study of the attacker’s profit, cost of attacking, defender’s utility payoff and the cost of defense are estimated using fuzzy logic theory and the game is analyzed for equilibrium. The fuzzy logic model is implemented using test values and the overall attacker’s payoff and the defender’s utility is estimated.

4.2 Calculating Attacker’s Payoff

For calculating the attacker’s payoff, we use fuzzy logic. We employ the rules described in Section 3 and we follow the Mamdani method in obtaining the profit estimate using fuzzy sets. The inputs are criticality of information and the damage that the attacker causes to the network as a result of the attack. Substituting the values obtained from the previous section, we get:

\[
\text{Criticality } X = [ \mu_{A1 = 0.25}, \mu_{A2 = 0.1}, \mu_{A3 = 0} ]
\]

\[
\text{Damage } Y = [ \mu_{B1 = 0.7}, \mu_{B2 = 0}, \mu_{B3 = 0} ]
\]

The crisp input \( r = 77 \) (criticality) corresponds to the membership functions \( A1 \) and \( A2 \) (criticality is high and moderate) to the degrees of 0.25 and 0.1 respectively.
The crisp input \( s=90 \) (damage) corresponds to the membership function \( B_1 \) only (damage is catastrophic) to the degree 0.7.

Also,

\[
\text{Profit } P = \frac{(0+10+20) \cdot 0 + (30+40+50+60+70) \cdot 0.1 + (80+90+100) \cdot 0.25}{(3 \cdot 0) + (5 \cdot 0.1) + (3 \cdot 0.25)}
\]

\text{Profit} = 74 \text{ (The profit value in the given universe of discourse (0 to 100) is 74)}

Therefore, using fuzzy sets and fuzzy logic, we calculated the profit to the attacker to be 74.

4.3 Calculating Defender’s Utility Payoff

For calculating the defender’s utility, we use fuzzy logic. We employ the rules described in Section 3 and we follow the Mamdani method in obtaining the utility estimate using fuzzy sets. The inputs are criticality of information and the level of threat the attacker causes to the network as a result of the attack.

\[
\text{Criticality } X = [ \mu (A_1 = 0.25), \mu (A_2 = 0.1), \mu (A_3 = 0) ]
\]

\[
\text{Damage } Y = [ \mu (B_1 = 0), \mu (B_2 = 0.5), \mu (B_3 = 0) ]
\]

The crisp input \( r=77 \) (criticality) corresponds to the membership functions \( A_1 \) and \( A_2 \) (criticality is high and moderate) to the degrees of 0.25 and 0.1 respectively. The crisp input \( s=65 \) (threat) corresponds to the membership function \( B_2 \) only (threat is moderate) to the degree 0.5.

\[
\text{Utility } U = \frac{(0+10+20) \cdot 0.25 + (30+40+50+60+70) \cdot 0.5 + (80+90+100) \cdot 0}{(3 \cdot 0.25) + (5 \cdot 0.5) + (3 \cdot 0)}
\]

\text{Utility} = 41 \text{ (The defender’s utility value in the given universe of discourse (0 to 100) is 41)}
Therefore, using fuzzy sets and fuzzy logic, we calculated the utility of the defender to be 41.

4.4 Measuring Threat and Damage to the Network

Threat:

The threat caused to the network can be expressed as a function of the following parameters [14]:

- Rating of Threat: $R_v$

$$R_v = a_v \times b_v$$

- Exploitability of Threat ‘v’, $a_v$ is the number of v’s causes in the network. Causes of the threat in the network are the ways that the threat can be converted into a complete attack.

- Effect of Threat ‘v’, $b_v$ is the number of v’s results in the network. Results in the network are the failure states that are created when a threat is converted into a complete attack.

- Depth ($v_i$) reflects the minimum number of steps an attacker takes to exploit the threat ‘v’.

- Active Threats - A threat is active; if the threat is converted to a complete attack

- Quiescent Threats - A threat is quiescent if there is no attack.

Active Threats:

$$A_v = \frac{\alpha \cdot R_v}{depth(v)}$$
Quiescent Threats

\[ Q_v = (1 - \alpha) \cdot R_v \]

\( \alpha \) is the weight associated with active threats.

The metric estimate for the threat to the network ‘\( M \)’ is the sum of all the active and quiescent threats in the network.

\[
M = \sum_{i=1}^{k} A_{vi} + \sum_{i=k+1}^{n} Q_{vi}.
\]

\[
= \alpha \sum_{i=1}^{k} \frac{R_{vi}}{\text{depth}(vi)} + (1 - \alpha) \sum_{i=k+1}^{n} R_{vi}.
\]

Damage

The amount of damage caused to the network can be obtained from the use of metrics according to the paper [15].

Metrics Used for the Denial of Service Attack

- Percentage of failed transactions (pft)– captures the impact of DoS attack on a network

- Dos-Hist – Specific application’s resilience to an attack

- Dos-Level – Weighted Average of pft measures of all applications

- QoS Ratio – ratio of difference between transaction’s traffic and threshold

- Failure Ratio – percentage of live transactions that may fail in the future
Why Fuzzy Logic for Estimation

The above metrics give a measure of the threat and damage to the network. A worst case analysis of the potential damage that can be inflicted can be realized by mapping the threat model to the damage model. This is for future work. However these metrics provide a base line to calculate damage or threat. The actual threat or damage cannot be determined as it depends in the capabilities of the attacker, his motivation etc. Hence these measurements are the most likely scenarios in our proposed fuzzy logic scheme that is, highest membership. Historical data, IDS information and other factors may be used to determine the spread in the fuzzy logic scheme.

4.5 Fuzzy Logic for the Cost of Attacking and the Cost of Defending

Similarly using fuzzy logic, we calculated the cost of defense $C_D$ to be 10

The cost of attacking $C_A (c1, c2)$ are 20, 30 respectively.

4.6 Net Profit to the Attacker for the given Fuzzy Logic Estimated Values:

$$P - C_A (c1 + c2) = 74 - (20 + 30) = 74 - 50 = 24;$$

$$P - c1 = 74 - 20 = 54$$

4.7 Net Utility to the Defender for the given Fuzzy Logic Estimated Values:

$$U - C_D = 41 - 10 = 31$$
4.8 Payoff Matrix with Numerical Estimates:

Substituting the numerical estimates obtained from the fuzzy logic theory into the payoff matrix, we get the following matrix.

<table>
<thead>
<tr>
<th>Defenders</th>
<th>Detected and Deceive</th>
<th>Undetected/No Deception</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attacker</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td>24, 31</td>
<td>54, 0</td>
</tr>
<tr>
<td>No Attack</td>
<td>0, 1</td>
<td>0, 0</td>
</tr>
</tbody>
</table>

Table 4.1 Payoff matrix with Numerical Estimates

4.9 Mixed Strategy Equilibrium of the Game:

Formally, a mixed strategy is a strategy profile that associates to each available action, a likelihood of being selected. In the theory of games, a player is said to use a mixed strategy whenever he or she chooses to randomize over the set of available actions. The intelligent attacker tries to launch a successful attack by employing strategies and updating its beliefs about the history of the game. But the defender can only observe the outcome of the game when the attack is detected. Hence the defender tries to maximize his payoff by trying to detect the attack and then consequently deceive the attacker. So no
player is selecting only one pure strategy, There is a mixture of strategies available to the players and each player tries to maximize his payoff by selecting the strategy that maximizes his payoff. Hence this game has mixed strategy equilibrium.

In a non-dynamic game, a strategy profile is a perfect pure strategy equilibrium if every strategy in that profile is a best response to every other strategy in the profile; i.e., there is no strategy that a player could play that would yield a higher payoff, given all the strategies played by the other players. Here, in our model, no strategy yields the highest payoff for both players together. Hence there is no perfect pure strategy equilibrium.

The objective of our game model is to maximize the defender’s payoff and to minimize the attacker’s payoff. Thus from the payoff matrix, it is evident that the strategy {Attack, Deceive} is the one that yields the highest payoff to the defender while at the same time minimizing the attacker’s payoff by a large value. Hence the game has mixed strategy equilibrium under the strategy {Attack, Deceive}. This equilibrium is termed Mixed Strategy Equilibrium since it is not a Perfect Pure Strategy Equilibrium.

4.10 Sample Game Play

A sample game play can be depicted as shown in the following figure. The attacker’s decisions and the defender’s decisions during the game play are shown in the form of strategies employed by the two players.
In game theory, the best strategy of a player will be one of the strategies from his strategy space that yields the highest payoff to that player. Here as we can see from the payoff matrix above, the best strategy to the defender is to always deceive the attacker since it yields a payoff of 31 to the defender as opposed to other payoffs which are 0, 1 and 0. The best strategy for the attacker is to always launch an attack rather than not...
launching an attack since the strategy of attack yields a payoff of 24 and 54 as opposed to 0 and 0 to the attacker.
CHAPTER V

CONCLUSION

5.1 Conclusion

In this thesis work, an attacker and defender model integrated with game theoretic approach is investigated for securing a sensor network. A new methodology using fuzzy logic has been introduced to effectively calculate and estimate the numerical values for the attacker’s and defender’s payoff functions. The cost of deception incurred to the defender as a result of employing deception as the defense mechanism has been analyzed. The cost of attacking incurred to the attacker as a result of the attack is also analyzed. In the proposed game model, each player tries to maximize his payoff. The attacker seeks to inflict the most damage without being detected while the defender tries to protect the network and maximize his payoff using deception. The main focus of this thesis was to propose a game structure that allows the defender to observe some of the attacker’s moves and detect if there is an attack. If the defender detects that there is an attack, the defender has to employ a deception mechanism so as to inflict the most damage to the attacker and thus effectively secure the network. A sample game play has been studied and a sample case study for the parameters has been analyzed. The payoff definition and the equilibrium for this game have been effectively implemented. This game model deception based security framework for sensor networks will reduce the computational
complexities and resource scarcity in sensor networks. There are many metrics which are used to measure threat and damage to the network but no numerical estimate is described for the metrics. Our contribution to this work is that we analyzed a game model to secure a sensor network and we used fuzzy logic to obtain a numerical estimate for the parameters. Our thesis work using fuzzy logic theory can be extended to focus on more generalized networks and can also be extended to analyze more metrics for measuring parameters like criticality, threat, damage and cost associated with the model. Future work in this area may focus on more sophisticated means of securing the sensor network by taking more parameters into consideration while calculating the payoffs and equilibrium strategies. Future work may also include modeling the game and analyzing the payoffs for a typical sensor network attack like a sinkhole attack.
REFERENCES


VITA

RENUKA KANDREGULA

Candidate for the Degree of

Master of Science

Thesis: GAME THEORY BASED DECEPTION FOR SECURITY IN NETWORKS

Major Field: Computer Science

Biographical:

Personal Data:
Born on April 16, 1985, Andhra Pradesh, India

Education:
- Completed the requirements for the Master of Science in Computer Science at Oklahoma State University, Stillwater, Oklahoma in May 2010.
- Bachelor of Engineering in Computer Science at Anna University, Chennai, India in April 2006.

Experience:
- Graduate Secretary, Computer Science Department, Oklahoma State University
- Research Analyst, Computer Science Department, Oklahoma State University
- Teaching Assistant, Computer Science Department, Oklahoma State University
- Software Developer, Anjana Software Solutions Inc, Chennai, India
Name: RENUKA KANDREGULA

Institution: Oklahoma State University

Title of Study: GAME THEORY BASED DECEPTION FOR SECURITY IN NETWORKS

Pages in Study: 41

Major Field: Computer Science

Scope and Method of Study:

In contrast to the complex techniques to secure a network which involve computation and communication overhead, a game theoretic based deception model is proposed in this thesis work. A game model with two players is studied and investigated for securing a network. A new methodology using fuzzy logic has been introduced to effectively calculate, estimate and quantify the values for the attacker’s and defender’s payoff functions. The cost functions incurred to the attacker and defender have also been analyzed. In the proposed game model, each player tries to maximize his payoff. The attacker seeks to inflict the most damage without being detected while the defender tries to protect the network and maximize his payoff using deception techniques.

Findings and Conclusions:

The main focus of this thesis was to propose a game structure that allows the defender to observe some of the attacker’s moves and detect if there is an attack. If the defender detects that there is an attack, the defender has to employ a deception mechanism so as to inflict the most damage to the attacker and thus effectively secure the network. A sample game play has been studied and a sample case study for the quantification of parameters has been analyzed using fuzzy logic theory. The payoff definition and the equilibrium for this game model have been effectively implemented. This game theory based deception security framework will reduce the computational complexities and hence helps in effectively securing the network.

ADVISER’S APPROVAL: Dr. Johnson P Thomas