A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks*

Animesh Patcha and Jung-Min Park
(Corresponding author: Animesh Patcha)

Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University
Blacksburg, VA 24061, USA (Email: apatcha@vt.edu)

(Received Sep. 4, 2005; revised and accepted Oct. 6, 2005)

Abstract

Nodes in a mobile ad hoc network need to thwart various attacks and malicious activities. This is especially true for the ad hoc environment where there is a total lack of centralized or third-party authentication and security architectures. This paper presents a game-theoretic model to analyze intrusion detection in mobile ad hoc networks. We use game theory to model the interactions between the nodes of an ad hoc network. We view the interaction between an attacker and an individual node as a two player non-cooperative game, and construct models for such a game.

Keywords: Intrusion detection, game theory, mobile Ad hoc networks

1 Introduction

In the past couple of years, considerable interest has developed in creating new kinds of network applications that fully exploit distributed mobile computing, particularly for military and defence purposes. The key underlying technology for such applications is the mobile ad hoc network (MANET).

MANETs, as the name suggests, have no supporting infrastructure. They are autonomous distributed systems that are comprised of a number of mobile nodes connected by wireless links, forming arbitrary time-varying wireless network topologies. Mobile nodes function both as hosts and routers. As hosts, they represent source and destination nodes in the network, while as routers, they represent intermediate nodes between a source and a destination, providing store-and-forward services to neighboring nodes. Store-and-forward services are needed due to the limited range of each individual mobile host's wireless transmission. Nodes that constitute the wireless network infrastructure are free to move randomly and organize themselves arbitrarily. Applications such as military exercises and disaster relief will benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications.

Flexibility and adaptability, which are the strengths of MANET, are unfortunately accompanied by increased security risks. Security in the MANET environment is particularly difficult to achieve, notably because of the limited physical protection to each of the nodes, the sporadic nature of connectivity, the absence of a certification authority, and the lack of a centralized monitoring or management unit. Intrusion prevention is not guaranteed to work all the time, and this clearly underscores the need for intrusion detection as a front–line security research area under the umbrella of ad hoc network security. In traditional wireless networks, mobile devices associate themselves with an access point which is in turn connected to other wired machines such as a gateway or a name server which handle network management functions. Ad hoc networks, on the other hand, do not use such access points and form a completely distributed architecture. The absence of an infrastructure and subsequently the absence of authorization facilities impedes the usual practice of establishing a line of defense—distinguishing nodes as trusted or non-trusted. There may be no ground for an *a priori* classification, since all nodes are required to cooperate in supporting the network operation and no prior security association (SA) can be assumed for all the network nodes. Freely roaming nodes form transient associations with their neighbors: they join and leave subdomains independently with and without notice.

In MANETs, compromised nodes may cause potential Byzantine failures in the routing protocols. In a Byzantine failure, a set of the nodes could be compromised in such a way that incorrect and malicious behavior cannot be detected. Malicious nodes can inflict a Byzantine failure on a system by creating new routing messages, advertising non-existent links or providing incrrect link

*A preliminary version of portions of this material was presented at the Fifth Annual IEEE Information Assurance Workshop, United States Military Academy, West Point, New York, June 2004.

state information. It can therefore be seen that intrusion prevention measures, like a firewall in MANETs are not enough.

Intrusion detection techniques are widely used in wired networks to protect networked systems. Intrusion detection techniques geared towards wired networks cannot, however, be applied directly to MANETs. This is especially because of the latter's lack of a fixed infrastructure, mobility, the vulnerability of wireless transmissions to eavesdropping and the lack of a clear separation between normal and abnormal behavior of the nodes. In addition, the ad hoc networking paradigm does not allow for the presence of traffic concentration points in the network, whereas most conventional intrusion detection systems (IDS) geared towards wired networks depend on such an architecture.

In this paper, we concentrate on providing a mathematical framework for intrusion detection in mobile ad hoc networks. We describe how game theory can be used to find strategies for both the malicious node and the administrator of the target node.

The organization of the paper is as follows. In Section 2 we briefly describe the related work. Section 2 is followed by Section 3, where we give a brief introduction to the concepts of game theory and introduce the formal model for non-cooperative games. We also relate the elements in the model to the problem at hand. In Section 4, we present our model for intrusion detection in a MANET. We conclude the paper in Section 5.

2 Related Work

IDS are classified as *anomaly detection* systems or *misuse detection* systems. The research in IDS's began with a report by Anderson [4] followed by a seminal paper by Denning [6]. Since then various models for intrusion detection have been proposed for wired networks. All existing approaches take into consideration domain specific knowledge to build suitable detection systems.

Research in IDSs for wireless networks, especially MANETs, is an emerging area that has a relatively short history. Marti *et al.* [12] introduced the concept of *Watchdog* and *Pathrater* to snoop promiscuously in the neighborhood of a given wireless node to identify routing misbehavior. However, the approach is prone to many false positives and is vulnerable to attacks from two consecutive and colluding adversaries where the first adversarial node does not report that the second did not forward the data successfully. Buchegger and Boudec [18] extended the work of Marti *et al.* by replacing the *Watchdog* with a *Neighborhood Watch* paradigm. In this paradigm, a node monitors the activities of its downstream neighbor. The authors in [18] also introduce a *Trust Manager*, a *Reputation System* and a *Path Manager*. The basic premise in their system is that each node runs a finite state machine to calculate the "trust" it has in its neighbor, which in turn is used to rank the other node's reputation. The path with the highest security metric is always chosen, and nodes with low reputation values are ignored and/or isolated from the system.

Zhang and Lee [20] put forth the basic requirements for an IDS in the MANET environment. They also proposed a general intrusion detection and response mechanism for MANETs, in which each IDS agent participates in the intrusion detection and response tasks independently. Huang *et al.* [8] extended the work done by Zhang and Lee. They use cross-feature analysis to analyze the routing activities and improve the anomaly detection process by providing more details about the attack types and attack sources. Sun *et al.* [19], proposed a Markov chain-based anomaly detection approach for MANETs.

The use of mobile agents in the context of IDS has also been proposed in the last couple of years. Kachirski and Guha [9] have proposed a distributed IDS for the MANET environment. The authors, use clustering to efficiently select a single layer of nodes that partially or completely cover all the links in the ad hoc network. Mobile agents are then used to send code for intrusion detection to these sparsely positioned nodes. Sparsely populated nodes are used to reduce the number of nodes required for effective intrusion detection while still being able to cover a wider area. In addition, by efficiently merging audit data from multiple network sensors, their bandwidth-conscious scheme analyzes the entire ad hoc wireless network for intrusions, thwarts intrusion attempts, and provides a lightweight low-overhead mechanism based on the mobile agent concept. However, promiscuous monitoring is not well suited for detecting attacks on conventional network and higher-layer protocols in MANETs. Two other notable research projects in the application area of mobile agents for intrusion detection are the LIDS project [16] and the SPARTA project [11]. For further information on intrusion detection for MANETs the reader is directed to the survey article in [14].

Game theory has been used extensively in computer and communication networks to model a variety of problems. The relevant body of work includes the work of Shenker [17] for modeling service disciplines, the work of Akella *et al.* [1] for TCP performance, and the work of Baser *et al.* [3] for modeling power control in a multi-cell wireless network. Bencsáth *et al.* [5] applied game theory and client puzzles to devise a defense against denial of service (DoS) attacks. In the area of MANETs, Michiardi *et al.* [13] used cooperative and non-cooperative game theoretic constructs to develop a reputation based architecture for enforcing cooperation.

Modeling intrusion detection using game theory, however, is a relatively new approach. Kodialam *et al.* [10] used a game theoretic framework to model intrusion detection via sampling in communications networks and developed sampling schemes that are optimal in the game theoretic setting. Our work is more closely related to the model proposed by Alpcan *et al.* [2]. We have extended the model proposed in [2] to include MANETs, and have analyzed the interaction between an attacker and a host-

based IDS as a dynamic two player non-cooperative game.

3 Game Theory

Game theory is a branch of applied mathematics that uses models to study interactions with formalized incentive structures ("games"). It has applications in a variety of fields, including economics, international relations, evolutionary biology, political science, and military strategy. Game theory provides us with tools to study situations of conflict and cooperation. Such a situation exists when two or more decision makers who have different objectives act on the same system or share the same set of resources. Therefore, game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. Some of the assumptions that one makes while formulating a game are:

1) There are at least two players in a game and each player has, available to him/her, two or more well-specified choices or sequences of choices.

2) Every possible combination of plays available to the players leads to a well-defined end-state (win, loss, or draw) that terminates the game.

3) Associated with each possible outcome of the game is a collection of numerical payoffs, one to each player. These payoffs represent the value of the outcome to the different players.

4) All decision makers are rational; that is, each player, given two alternatives, will select the one that yields the greater payoff.

Game theory has been traditionally divided into *cooperative* game theory and *non-cooperative* game theory. The two branches of game theory differ in how they formalize interdependence among the players. In non-cooperative game theory, a game is a detailed model of all the moves available to the players. In contrast, cooperative game theory abstracts away from this level of detail and describes only the outcomes that result when the players come together in different combinations. In this paper, we consider non-cooperative games.

3.1 Non-Cooperative Game Theory

Non-cooperative game theory studies situations in which a number of nodes/players are involved in an interactive process whose outcome is determined by the node's individual decisions and, in turn, affects the well-being of each node in a possibly different way.

Non-cooperative games can be classified into a few categories based on several criteria. Non-cooperative games can be classified as *static* or *dynamic* based on whether the moves made by the players are simultaneous or not. In a *static game*, players make their strategy choices simultaneously, without the knowledge of what the other players are choosing. Static games are generally represented diagrammatically using a game table that is called the *normal form* or *strategic form* of a game. In contrast, in a *dynamic game*, there is a strict order of play. Players take turns to make their moves, and they know the moves played by players who have gone before them. *Game trees* are used to depict dynamic games. This methodology is generally referred to as the *extensive form* of a game. A game tree illustrates all of the possible actions that can be taken by all of the players. It also indicates all of the possible outcomes at each step of the game.

Non-cooperative games can also be classified as *complete information* games or *incomplete information* games, based on whether the players have complete or incomplete information about their adversaries in the game. Here *information* denotes the payoff-relevant characteristics of the adversaries. In a *complete information* game, each player has complete knowledge about his/her adversary's characteristics, strategy spaces, payoff functions, and so on. For further details on game theory, the reader is directed to [7, 15].

In this paper, we model the interaction between an attacker and an intrusion detection system as a *basic signaling game* which falls under the gambit of *multi-stage dynamic non-cooperative game with incomplete information.* As mentioned above, in a non-cooperative game *with incomplete information*, we model situations in which some players have some private information before the beginning of a game. This initial private information is called the *type* of a player and it fully describes any information the player has, which is not common knowledge. A player may have several types, one for each possible state of his/her private information. It is also assumed that each player knows his/her own type with complete certainty.

3.2 Basic Signaling Game

A basic signaling game, in its simplest form has two players—Player 1 who is the sender and Player 2 who is the receiver. For the sake of convenience we treat Player 1 as masculine and Player 2 as feminine. Nature[1] draws the type of the sender from a type set Θ, whose typical element is θ. The type information is private to each sender. Player 1 observes information about his type θ and chooses an action a_1 from his action space A_1. Player 2, whose type is known to everyone observes a_1 and chooses an action a_2 from her action space A_2. Player 2 has prior beliefs, before the start of the game, about Player 1's type. In other words, before observing the sender's message, the receiver believes that the probability that the sender is some type $\theta \in \Theta$ is $p(\theta)$. The action spaces of mixed actions are A_1 and A_2 with ele-

[1] We often want to include in our model some extrinsic uncertainty, that is some random event not under the control of the players. We indicate this by allowing nodes to be owned by an artificial player that we call "Nature" and sometimes index as Player 0. Nature's moves are not labeled in the same way as the moves of the strategic players. Rather we associate probabilities to each of nature's moves.

ments α_1 and α_2 respectively.

Player i's payoff is denoted by $u_i(\alpha_1, \alpha_2, \theta)$. Player 1's strategy is a probability distribution $\sigma_1(\cdot|\theta)$ over actions a_1 for each type θ . A strategy for Player 2 is a probability distribution $\sigma_2(\cdot|\alpha_1)$ over actions a_2 for each action a_1.

After both the players have taken their actions, the payoffs are awarded according to the *message* sent by the sender, the action taken by the receiver in response and the type θ of the sender chosen by Nature.

Type θ's payoff to strategy $\sigma_1(\cdot|\theta)$ when Player 2 plays $\sigma_2(\cdot|a_1)$ is

$$u_1(\sigma_1, \sigma_2, \theta) = \sum_{a_1} \sum_{a_2} \sigma_1(a_1|\theta)\sigma_2(a_2|a_1)u_1(a_1, a_2, \theta).$$

Player 2's payoff to strategy $\sigma_2(\cdot|a_1)$ when Player 1 plays $\sigma_1(\cdot|\theta)$ is

$$\sum_{\theta} p(\theta)(\sum_{a_1} \sum_{a_2} \sigma_1(a_1|\theta)\sigma_2(a_2|a_1)u_2(a_1, a_2, \theta)).$$

Player 2 updates her beliefs about θ and bases her choice of action a_2 on the posterior distribution[2] $\mu(\cdot|a_1)$ over Θ. *Bayesian Equilibrium* dictates that Player 1's action will depend on his type. Therefore, if $\sigma_1^*(\cdot|\theta)$ denotes this strategy, then knowing $\sigma_1^*(\cdot|\theta)$ and by observing a_1, Player 2 can use Bayes rule to update $p(\cdot)$ and $\mu(\cdot|a_1)$. Drew and Tirole [7] state that the natural extension of the subgame-perfect equilibrium[3] is the *perfect Bayesian equilibrium*, which requires Player 2 to maximize her payoff conditional on a_1 for each a_1.

Definition 1 *A perfect Bayesian equilibrium(PBE) of a signaling game is a strategy profile σ^* and posterior beliefs $\mu(\cdot|a_1)$ such that*

$$\mathrm{P}_1 : \forall\theta, \sigma_1^*(\cdot|\theta) \in \arg\max_{\alpha_1} \mathrm{u}_1(\alpha_1, \sigma_2^*, \theta)$$

$$\mathrm{P}_2 : \forall \mathrm{a}_1, \sigma_2^*(\cdot|\mathrm{a}_1) \in \arg\max_{\alpha_2} \sum_{\theta} \mu(\theta|\mathrm{a}_1)\, \mathrm{u}_2(\mathrm{a}_1, \alpha_2, \theta)$$

$$\mathrm{B} : \mu(\theta|\mathrm{a}_1) = \frac{\mathrm{p}(\theta)\sigma_1^*(\mathrm{a}_1|\theta)}{\sum_{\theta^1 \in \Theta} \mathrm{p}(\theta^1)\sigma_1^*(\mathrm{a}_1|\theta^1)}$$

if $\sum_{\theta' \in \Theta} p(\theta')\sigma_1^*(a_1|\theta') > 0$ and $\mu(\cdot|a_1)$ is any probability distribution on Θ if $\sum_{\theta' \in \Theta} p(\theta')\sigma_1^*(a_1|\theta') = 0$.

Where P_1 and P_2 are the perfection conditions and B corresponds to the application of Bayes rule. P_1 says that Player 1 takes into account the affect of a_1 on Player 2's action. P_2 states that Player 2 reacts optimally to Player 1's action given her posterior beliefs about θ. In other words, a perfect Bayesian equilibrium must satisfy the subgame perfection criterion and in addition the model must satisfy the following Bayesian postulates.

- For each information set, the players must have beliefs about the stage the game has reached.
- Whenever it is a players turn to move, his/her actions must be optimal from that point onwards given his/her beliefs.
- The players beliefs about neighboring nodes, must be determined using the Bayes rule.

Thus, a perfect Bayesian equilibrium can be thought of as a set of strategies and beliefs such that at any stage of the game, strategies are optimal given the beliefs. These beliefs are obtained from the equilibrium strategies and the observed actions using Bayes rule.

We believe that intrusion detection in MANETs can be modeled as a basic signaling game for a number of reasons. First and foremost, in a MANET environment, it is very hard to distinguish a friend from a foe in the absence of security mechanisms such as public key infrastructure(PKI), digital certificates, etc. Therefore, the *type* of a particular node is not easily verifiable by other nodes in the system. Secondly an IDS responds to the intrusion after an intrusion has occurred. Therefore, we believe that modeling intrusion detection in a game theoretic framework based on dynamic non-cooperative games is the right direction to take.

4 A Game Theoretic Model of Intrusion Detection

The very nature of MANETs, dictates that any IDS designed for such a network has to be distributed in nature. Centralized solutions that have a single point of failure cannot be used. Assuming a host based IDS, we model an intrusion detection game played between a host and an intruder.

In this section, we present our game theoretic framework to analyze and model the response of an IDS. Examples of IDS response actions include setting off an alarm, watching suspicious activity before setting off an alarm, and a total system reconfiguration.

We model the interaction between an attacker and a host based IDS as a two player signaling game which falls under the gambit of multi-stage dynamic non-cooperative game with incomplete information.

In the intrusion detection game, the objective of the attacker is to send a malicious message from some attack node with the intension of attacking the target node. The intrusion is deemed successful when the malicious message reaches the target machine without being detected by the host IDS. We assume that an intrusion is detected and

[2] In Bayesian inference, when we have performed an experiment we use Bayes' theorem to find a new distribution which reflects the result of the experiment. This new distribution is called the posterior distribution.

[3] In extensive-form games with complete information, many strategy profiles that form the best responses to one another imply incredible threats or promises that a player actually does not want to carry out anymore once he must face an (unexpected) off-equilibrium move by an opponent. If the profile of strategies is such that no player wants to amend his strategy whatever decision node can be reached during the play of the game, an equilibrium profile of strategies is called *subgame perfect*. In this sense, a subgame-perfect strategy profile is "time consistent" in that it remains an equilibrium in whatever truncation of the original game (subgame) the players may find themselves.

the intruding node is blocked when a message sent by a probable intruder is intercepted and the host IDS can say with certainty that the message is malicious in nature.

For an IDS, the basic performance criteria is the rate of false alarms in the system. There exists a tradeoff between the reduction in false alarms and the reduction of undetected intrusions — decreasing the system sensitivity to reduce the number of false alarm result in the increase of undetected intrusions. Either extremes are undesirable as the IDS becomes totally ineffective in such circumstances. In our system model, we consider the cost associated with an undetected intrusion to be much more severe than the cost associated with false alarms.

To simplify our analysis, we assume that a *malicious node* attacks only one node at a time and that collusion between malicious nodes do not occur. In addition, we do not consider selfish node[4] activity. The IDS does one of two things: it either sets off an alarm on detection of an intrusion or does nothing.

4.1 System Model

In our model of the signaling game, a node is the *sender* and the host based IDS based is the *receiver* to which the message is directed. The senders private information will be his nature. In other words, the sender node could be of two *types*: he could be a *regular node* or he could be a *malicious node/attacker*. The type space of a given sender is, therefore, given by $\Theta = [Attacker, RegularNode]$. The IDS prior beliefs concerning the probability that any other node in the system is either an *attacker* or a *regular node* can be described by a single number $q \in [0, 1]$.

The malicious node's (*attacker*) decision is a choice between exhibiting malicious behavior or exhibiting normal behavior. Let the probability of a particular malicious node exhibiting malicious activity be s, and the probability of the same node exhibiting normal behavior be $1 - s$. The particular choice that the attacker makes is his "message". The IDS "detects" this decision with a probability t and misses it with a probability $1 - t$ depending on his beliefs.

Consider the attacker-IDS game shown in Figure 1. Note that the sender has two information sets, corresponding to his two types (viz. Attacker and Normal Node). The receiver also has two information sets, but these correspond to the senders two possible messages (viz. defend and miss) rather than to the senders possible types. The IDS has a gain of $-\gamma_{defend}$ for detecting an attack where as there is a cost involved whenever the IDS misses an attack (γ_{miss}) or when it raises a false alarm (γ_{falarm}). On the other hand, the intruder has a gain of $-\delta_{intrude}$ on a successful undetected intrusion and a cost of δ_{caught} on being detected and blocked. False alarms have a zero cost value to the attacker. In this paper, we assume that the payoffs for the IDS and the node are different in the case of an active attack as compared to the payoffs awarded in the case of a passive attack. To illustrate this point, the payoffs awarded in the latter case are shown by $\overline{\gamma}$ and $\overline{\delta}$ in Figure 1.

For the attacker, in all possible cases, the expected payoff is

$$s[t\delta_{caught} - (1-t)\delta_{intrude}].$$

Similarly, for the IDS, in all possible cases, the expected payoff is

$$s\gamma_{miss} + t\gamma_{falarm} - st(\gamma_{defend} + \gamma_{falarm} + \gamma_{miss}).$$

A rational node will always try to maximize (7). If the cost of the false alarm (γ_{falarm}) is relatively low, then the IDS will always choose to sound an alarm. The *Nash equilibrium*[5] for such a signaling game is described by the following condition.

For the attacker/regular node: Given the strategy of the IDS, each type θ of a node evaluates the utility from sending a message a_1 as $\sum_{a_2} \sigma_2(a_2|a_1)u_1(a_1, a_2, \theta)$ and $p(\theta)$ puts weight on a_1 only if it is amongst the maximizing messages in this expected utility.

For the IDS: The IDS will proceed in two steps. First for every message a_1 that is sent with positive probability by some type θ, the IDS uses Bayes rule to compute the posterior probability assessment that a_1 comes from each type θ . According to the Nash equilibrium condition, for all a_1 that are sent by some type θ with positive probability, every response a_2 in support of the IDS's response should be the best response to a_1 given the beliefs that are computed using Bayes rule.

Therefore, we can say that the IDS strategy will be the best response to the sending nodes behavior strategy if and only if it maximizes its expected utility over all possible pure strategies. The strategy of the IDS will, therefore, be to pick the optimal strategy

$$\forall\theta, \sigma_1^*(\cdot|\theta) \ \in \arg\max_{\alpha_1} u_1(\alpha_1, \sigma_2^*, \theta),$$

out of its available set in response to a message a_1 from the sending node. The choice of strategy must be based on the receiver's prior beliefs such that it is able to maximize the effective payoff by minimizing the cost due to false alarms and missed attacks.

Bayes theorem being recursive in nature allows each node to periodically update its posterior beliefs about other nodes from its previous posterior distribution based on independent observations. Intuitively, we can see that

[4] Selfish nodes are nodes that use the network resources but act selfishly in order to save system resources like battery life for their own needs. They do not intend to directly damage other nodes

[5] A profile of strategies such that given the other players conform to the (hypothesized) equilibrium strategies, no player has an incentive to unilaterally deviate from his (hypothesized) equilibrium strategy. The self-reference in this definition can be made more explicit by saying that a Nash equilibrium is a profile of strategies that form "best responses" to one another, or a profile of strategies which are "optimal reactions" to "optimal reactions". Nash equilibrium is the pure form of the basic concept of strategic equilibrium; as such, it is useful mainly in normal form games with complete information. When allowing for randomized strategies, at least one Nash equilibrium exists in any game(unless the players' payoff functions are irregular); for an example, see the game of matching pennies in the entry on game theory. Typically, a game possess several Nash equilibria, and the number of these is odd.

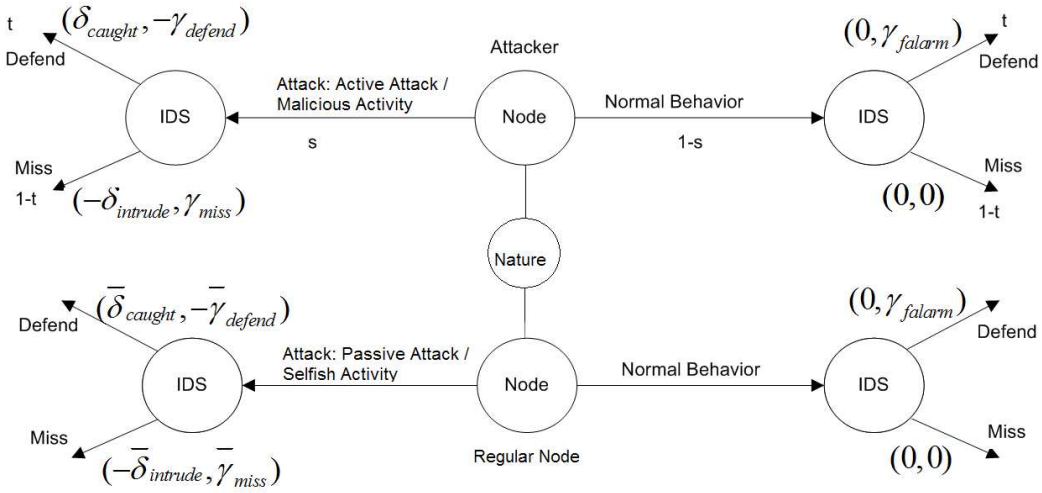

Figure 1: An attacker-IDS basic signaling game

with time the false alarm rates will decrease. When applied in tandem with other approaches like likelihood evaluation and active intruder profiling, the false alarm rates can be further reduced. A full explanation of these methods is beyond the scope of this paper.

The game theoretic investigation presented in this paper gives us valuable insight into the behavior of the attacker and the IDS. We believe that most of the simplifying assumptions made in this paper can be modified to incorporate more realistic scenarios.

5 Conclusions and Research Issues

Ad hoc network security has come into the lime light of network security research over the past couple of years. However, little has been done in terms of defining the security requirements specific to MANETs. Such security requirements must include countermeasures against node misbehavior and denial of service attacks. In this paper, we used the concept of multi-stage dynamic non-cooperative game with incomplete information to model intrusion detection in a network that uses a host-based IDS. As long as the beliefs are consistent with the information obtained and the actions are optimal given the beliefs, the model is theoretically consistent. We believe that this game-theoretic modeling technique models intrusion detection in a more realistic way compared to previous approaches. As part of our future work, we intend to extend our game theoretic approach to take into account selfish nodes and groups of colluding attackers.

References

[1] A. Akella, S. Seshan, R. Karp, S. Shenker, and C. Papadimitriou, "Selfish behavior and stability of the internet: a game-theoretic analysis of TCP," in *Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM 2002:)*, pp. 117–130, 2002.

[2] T. Alpacan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proceedings of 42rd IEEE Conference on Decision and Control*, pp. 1880–1889, Piscataway, NJ, USA, Dec. 2003.

[3] T. Alpcan, T. Basar, and S. Dey, "A power control game based on outage probabilities for multicell wireless data networks," in *Proceedings of the American Control Conference*, vol. 2, pp. 1661–1666, Piscataway, NJ, USA, July 2004.

[4] J. P. Anderson, *Computer Security Threat Monitoring and Surveillance*, Technical Report, Contract 79F26400, James P. Anderson Co., Fort Washington, Fort Washington, PA, 1980.

[5] B. Bencsath, I. Vajda, and L. Buttyan, "A game based analysis of the client puzzle approach to defend against dos attacks," in *Proceedings of the IEEE Conference on Software, Telecommunications and Computer Networks*, pp. 763–767, 2003.

[6] D. E. Denning, "An intrusion detection model," in *IEEE Transactions on Software Engineering*, vol. 13, pp. 222–232, Piscataway, NJ, USA, 1986.

[7] D. Fudenberg and J. Tirole, *Game Theory.* Cambridge, MA: The MIT Press, 2002.

[8] Y. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies," in *Proceedings of the 23rd International Conference on Distributed Computing Systems (ICDCS 2003:)*, pp. 478–487, 2003.

[9] O. Kachirski and R. K Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *Proceedings of the IEEE Workshop on Knowl-*

edge Media Networking, pp. 153–158, Piscataway, NJ, USA, July 2002.

[10] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: A game theoretic approach," in *IEEE INFOCOMM 2003*, pp. 1880–1889, Piscataway, NJ, USA, Apr. 2003.

[11] C. Kruegel and T. Toth, "Flexible, mobile agent based intrusion detection for dynamic networks," Technical Report TUV-1841-2002-27, Distributed Systems Group at the Technical University of Vienna, 3rd Floor, Central Entrance, 1040 Vienna, Austria, Apr. 30 2002.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking (ACM MobiCom 2000:)*, pp. 255–265, New York, NY, USA, 2000.

[13] P. Michiardi and R. Molva, "COREe: A COllaborative REputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, pp. 107–121, Sep. 2002.

[14] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless Ad hoc networks," in *IEEE Wireless Communications*, vol. 11, pp. 48–60, Piscataway, NJ, USA, Feb. 2004.

[15] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. Cambridge, MA: The MIT Press, 1994.

[16] R. S. Puttini, J. M. Percher, L. Me, O. Camp, R. T. S. Jnior, C. J. B. Abbas, and L. J. Garca-Villalba, "A modular architecture for distributed IDS in MANET," in *Proceedings of the 2003 International Conference on Computational Science and Its Applications (ICCSA)*, LNCS 2669, pp. 91–113, Springer, May 2003.

[17] S. J. Shenker, "Making greed work in networks: a game-theoretic analysis of switch service disciplines," *IEEE/ACM Transactions of Networking*, vol. 3, no. 6, pp. 819–831, 1995.

[18] J. Y. L. B. Sonja Buchegger, "Nodes bearing grudges: towards routing security, fairness, and robustness in mobile Ad-hoc networks," in *Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pp. 403–410, Washington, DC, USA, 2002.

[19] B. Sun, K. Wu, and U. Pooch, "Routing anomaly detection in mobile Ad-hoc networks," in *Proceedings of the 12th International Conference on Computer Communications and Networks (ICCCN 03)*, pp. 25–31, Piscataway, NJ, USA, 2003.

[20] Y. Zhang and W. Lee, "Intrusion detection in wireless Ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking (ACM MOBICOM 2000)*, pp. 275–283, New York, NY, USA, 2000.

Animesh Patcha is a doctoral candidate in the Bradley Department of Electrical and Computer Engineering at Virginia Tech since August 2002. His area of research is computer and network security in wired and wireless networks. Currently he is working on stochastic intrusion detection techniques under the expert guidance of Dr Jung-Min Park. Prior to coming to Virginia Tech, Animesh received his M.S. degree in Computer Engineering from Illinois Institute of Technology, Chicago,IL in May 2002 and his B.E. in Electrical and Electronics Engineering from Birla Institute of Technology Mesra, Ranchi, India in December 1998 respectively. From January 1999 to December 2000, he was a software engineer at Zensar Technologies in Pune, India. He is currently a student member of the IEEE and ASEE.

Jung-Min Park received the B.S. and M.S. degrees both in electronic engineering from Yonsei University, Seoul, South Korea, in 1995 and 1997, respectively; and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, in 2003. He is currently an Assistant Professor in the Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA. From 1997 to 1998, he worked as a cellular systems engineer at Motorola Korea Inc. His current interests are in network security, applied cryptography, and networking. More details about his research interests and publications can be found at http://www.ecpe.vt.edu/faculty/park.html. Dr. Park is a member of the Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), and the Korean-American Scientists and Engineers Association (KSEA). He was a recipient of a 1998 AT&T Leadership Award.