

# Modelling Bayesian attacker detection game in wireless networks with epistemic logic

Oldooz Dianat  
Department of Computing  
Macquarie University  
Sydney, NSW 2109, Australia  
Email: oldooz.dianat@mq.edu.au

Mehmet Orgun  
Department of Computing  
Macquarie University  
Sydney, NSW 2109, Australia  
Email: mehmet.orgun@mq.edu.au

**Abstract**—In collaborative networks operating over a wireless medium, to maximize connectivity of the network, two nodes that are not directly connected may need to communicate with one another through other nodes in the network. However in such networks, not all nodes are reliable. Therefore it may be necessary for legitimate users to monitor the behavior of other nodes such that they can form a belief about whether those nodes are potential attackers or not. These beliefs can be studied precisely in game theoretic scenarios such as Bayesian attacker detection games. These games are strategic games with incomplete information for modeling the interaction between nodes in wireless networks with channel uncertainty. However these games do not normally consider the reasoning abilities of agents. One solution is to use formal logics which allow for modeling the reasoning abilities of agents as well as allowing formal reasoning about certain properties of games such as the Nash equilibrium. In this paper, we propose an epistemic logic to study strategic games with incomplete information. In this logic we can precisely describe what the requirements and consequences of informative actions are. We can reason what rational agents should do if they can choose between different available actions. In addition, this language can be used as a semantically well-defined query language for model checkers to automatically verify the game descriptions with respect to their intended specifications.

**Index Terms**—Bayesian games, epistemic logic, wireless network security.

## I. INTRODUCTION

Wireless networks cover a wide spectrum of architectures such as wireless metropolitan mesh networks, sensor networks and ad hoc networks [1]. Collaboration in these networks improves the connectivity [2], for example with an ad hoc network, the number of sensor nodes can collaboratively collect information and then collaboratively send the information back [3]. However since in these networks collaborative nodes are responsible for all functions such as packet forwarding, routing and network management, they are sensitive to the misbehavior of nodes. The nodes' misbehaviors that affect these operations may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks aiming at denial of service (DoS) [4]. Here we focus on nodes that are attackers. While advanced cryptographic techniques can be used, the security challenges, e.g., DoS attacks, in wireless networks are not fully addressed because of the distributed nature of the networks. Hence, it is desirable

that security schemes can be modeled from nodes' perspective. Wang et al [5] used game theory to capture and analyze the interaction between an attacker and a regular node in wireless networks. They modeled the scenario as Bayesian attacker detection games, in which nodes have imperfect information because the attacker can disguise as a regular node and the actions are hidden because of the noise and imperfect observation.

Games with incomplete information or Bayesian games such as Bayesian attacker detection games provide a natural and compelling model that enables understanding actions of players under uncertainty. However these models do not provide any mechanisms for players (nodes) to reason about different situations in these models. One solution is to use formal logics for these models. The positive aspects of logic approaches are that we can specify the properties of agents and multi-agent systems as logical axioms and theorems in the language with clear semantics. Therefore there is no ambiguity in the specification and everything is explicit. Furthermore, properties, interrelationships and inferences are open to examination. In comparison to logic, computer programs need implementation and control aspects within. Thus the issues, which are to be tested, can often become confusing [6].

The aim of this paper is to represent and reason about Bayesian attacker detection games using formal logics. We develop a formal language for representing Bayesian games. There are several approaches for considering uncertainty in a logic that involves the quantification of uncertainty [7]. In this paper, we use beliefs about uncertainty to model Bayesian games. The logic for Bayesian games is the extension of the epistemic logic for normal form games and our work has been inspired from [8] and [9]. We introduce several special propositions and axioms to model Bayesian games. We also apply the extended logic to model a Bayesian game. We then illustrate reasoning for the solution concept in this game.

The structure of this paper is as follows. First, we present the syntax and the semantics of the extended epistemic logic for Bayesian games. Next is modeling Bayesian attacker detection games by this logic. Following, we use the logic for reasoning about the solution concept of these games. The paper concludes with a summary and discussion of future work.

## II. EPISTEMIC LOGIC FOR BAYESIAN GAMES

Bayesian games model those situations in which the game being played is not common knowledge. Instead, some players may hold a different payoff table or pure strategy set to be true. In a Bayesian game a player's beliefs include his knowledge of the game description (payoffs, strategies), as well as the probability distribution over the beliefs other agents may have. The set of beliefs held by a player is known as his epistemic type or simply type. The uncertainty is defined directly over a game's utility function. Therefore a Bayesian game is a tuple  $(N, S, \Theta, p, u)$  where:

- $N$  is a finite set of  $n$  players, indexed by  $i$ .
- $S = S_1 \times \dots \times S_n$  where  $S_i$  is a finite set of strategies of player  $i$ .
- $\Theta = \Theta_1 \times \dots \times \Theta_n$ , where  $\Theta_i$  is the type space of player  $i$ .
- $p : \Theta \rightarrow [0, 1]$  is a common prior over types.
- $u = (u_1, \dots, u_n)$  where  $u_i : S \times \Theta \rightarrow R$  is a real-valued utility (or payoff) function for player  $i$ .

The assumption is that all the above is common knowledge among the players, and each agent knows his own type.

In this section we propose an epistemic logic for representing and reasoning about Bayesian games.

The logical symbols used are  $\neg$  (negation),  $\wedge$  (conjunction),  $\vee$  (disjunction), (implication), and  $\leftrightarrow$  (equivalence). The conjunction (disjunction) of all sentences from a finite set  $\Sigma$  is abbreviated by  $\bigwedge \Sigma$  ( $\bigvee \Sigma$ ), assuming commutativity. If the  $\varphi_i$  enumerate  $\Sigma$  we may also write  $\bigwedge_i \varphi_i$  ( $\bigvee_i \varphi_i$ ). Before we go through the propositions and axioms of the epistemic logic, we should give a clear meaning for notation  $\theta_{n_i}$ . This notation denotes a set of types for player  $i$ , which means:  $\theta_{n_i} = \{\theta_{i,1}, \theta_{i,2}, \dots, \theta_{i,n}\}$ . In this definition  $\theta_{n_i}$  says that player  $i$  has  $n$  different types. The other critical notation is  $\theta_{n_i, n(-i)}$  that describes a set of types for player  $i$  in combination with other players' types. The language has a knowledge operator  $K_i$ , one for each agent  $i \in N$ . Basic propositions are:

- The proposition letters  $\mathbf{i}_{m\theta_{n_i}}$  stand for the statement ' $i$  plays his  $m$ th strategy in his  $\theta_{n_i}$  type'.
- The proposition  $\mathbf{u}_i(1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}) = \mathbf{r}_{i,1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}}$  denotes that the utility for player  $i$  with type  $\theta_{n_i}$ , when the strategy profile  $(1_{k_1}, \dots, N_{k_N})$  is played in combination with other players types  $\theta_{n(-i)}$ , equals the number  $r$ .
- $R$  is a set of countably many symbols such as  $r$ . The elements of  $R$  represent real numbers. In other words,  $R$  is a countable subset of the set of real numbers.
- The proposition  $\mathbf{r}_{i,1_{k_1}, \dots, i_m, \dots, N_{k_N} \succeq \mathbf{r}_{i,1_{k_1}, \dots, i_n, \dots, N_{k_N}}$  states that for player  $i$  his  $m$ th strategy is at least as good as his  $n$ th strategy.
- The proposition **rattype** $_i$  denotes the rationality of player  $i$ , in the sense that  $i$  is an expected utility maximizer.

We use the syntax introduced by [10] for probabilistic expressions.  $\mathbf{P}_i(\cdot)$  represents  $i$ 's probabilistic belief of player  $i$ 's type and arbitrary finite sums of such expressions

$\mathbf{P}_i(\varphi_1) \cdot \mathbf{q}_1 + \dots + \mathbf{P}_i(\varphi_n) \cdot \mathbf{q}_n \geq \mathbf{q}$  are allowed as long as they are not mixed over players (as  $\mathbf{P}_i(\varphi_1) \cdot \mathbf{q}_1 + \mathbf{P}_j(\varphi_2) \cdot \mathbf{q}_2 \geq \mathbf{q}$  would be for  $i \neq j$ ), and obvious abbreviations use the  $\Sigma$  notation. In this work  $\varphi$  represents the type of players and  $q$  the payoffs.

To allow for probabilistic reasoning the Kolmogorov axioms are essential.

- NonNeg:  $\mathbf{P}_i(\varphi_1) \geq 0$ .
- True:  $\mathbf{P}_i(\top) = 1$ .
- False:  $\mathbf{P}_i(\perp) = 0$ .
- Add:  $\mathbf{P}_i(\varphi) = \mathbf{P}_i(\varphi \wedge \psi) + \mathbf{P}_i(\varphi \wedge \neg\psi)$ .
- Dist:  $\mathbf{P}_i(\varphi) = \mathbf{P}_i(\psi)$  whenever  $\varphi \leftrightarrow \psi$  is a propositional tautology.

In order to ensure that probabilistic and non-probabilistic beliefs are related in the right way, two additional axioms are useful [9].

- Cons:  $K_i\varphi \leftrightarrow \mathbf{P}_i(\varphi) = 1$ .
- KnProb:  $\varphi \rightarrow K_i\varphi$  for  $\varphi$  an  $i$ -probability sentence (the sentence starts with  $\mathbf{P}_i$  or Boolean combinations thereof).

Then there are specific axioms for Bayesian games.

$$\bigwedge_i \bigvee_m \mathbf{i}_{m\theta_{n_i}} \quad (G'1)$$

$$\bigwedge_i \bigwedge_m \neg(\mathbf{i}_{m\theta_{n_i}} \wedge \mathbf{i}_{n\theta_{n_i}}) \quad (G'2)$$

$$\bigwedge_i \bigwedge_m (K_i \mathbf{i}_{m\theta_{n_i}} \leftrightarrow \mathbf{i}_{m\theta_{n_i}}) \quad (G'3)$$

$$\mathbf{u}_i(1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}) = \mathbf{r} \rightarrow K_i \mathbf{u}_i(1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}) = \mathbf{r} \quad (G'4)$$

$$\begin{aligned} &(\mathbf{r}_{i,1_{k_1}, \dots, i_m, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}} \succeq \\ &\mathbf{r}_{i,1_{k_1}, \dots, i_n, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}}) \vee \\ &(\mathbf{r}_{i,1_{k_1}, \dots, i_n, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}} \succeq \\ &\mathbf{r}_{i,1_{k_1}, \dots, i_m, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}}) \end{aligned} \quad (G'5)$$

Axiom G'1 says that every player plays one strategy based on his type in each state. And G'2 states that a player cannot choose two strategies at each state. Axiom G'3 implies that every player knows his own strategies likewise G'4 says that every player knows its own utilities. The last axiom G'5 states that the ordering of strategies is complete.

The epistemic logic is a multi-modal logic with  $n$  operators  $K_1, K_2, \dots, K_n$  where for  $i = 1, \dots, n$ ,  $K_i\varphi$  means that player  $i$  knows that  $\varphi$ . On the semantic side we use Kripke structures  $\langle \Omega, \mathcal{K}_1, \dots, \mathcal{K}_n \rangle$  where  $\Omega$  is a set of states or possible worlds and for every  $i \in \{1, \dots, n\}$ ,  $\mathcal{K}_i$  is a binary accessibility relation on  $\Omega$ . For every  $w \in \Omega$  and for every  $i \in \{1, \dots, n\}$  let  $\mathcal{K}_i(w) = \{w' \in \Omega : w\mathcal{K}_i w'\}$ .

Given a game  $G = (N, \{S_i\}_{i \in N}, \{\Theta_i\}_{i \in N}, p, u)$  and a Kripke frame  $F = \langle \Omega, \{\mathcal{K}_i\}_{i \in N} \rangle$ , a frame for  $G$  is obtained by adding the following functions to  $F$ . These functions are  $\sigma_i : \Omega \rightarrow S_i$  ( $i \in N$ ) satisfying that if  $w' \in \mathcal{K}_i(w)$  then  $\sigma_i(w') = \sigma_i(w)$ . It is necessary to have the notation  $\sigma_{-i}(w)$  which is the strategy profile of the players other than  $i$ . In

this logic we have the formula  $\mathbf{P}_i(\varphi) \geq b$ , which means that "according to agent  $i$ , formula  $\varphi$  holds with probability of at least  $b$ ", where  $b$  is an arbitrary rational number. From probability theory [11] a probability space is a tuple  $(\Gamma, \mathcal{H}, \mu)$  where  $\Gamma$  is a set called a sample space,  $\mathcal{H}$  is a  $\sigma$ -algebra of subsets of  $\Gamma$ , whose elements are called measurable sets, and a probability measure  $\mu$  is defined on the elements of  $\mathcal{H}$ . Without loss of generality we assume that  $\Gamma = \mathcal{H}$ . Hence the other type of functions is  $\mathcal{P}_i$  which is a probability assignment that assigns to each player  $i$  and state  $w \in \Omega$  a probability space  $\mathcal{P}(i, w) = (\sigma_{i,w}, \mu_{i,w})$  where  $\sigma_{i,w} = \sigma_i(w)$  and  $\sigma_i(w) : \Omega \rightarrow \mu(S_i) (i \in N)$ .  $\mathcal{P}(i, w)$  can be considered as  $\Delta(\Omega)$  that denotes the set of probability distribution over  $\Omega$ . Therefore  $\mathcal{P}_i : \Omega \rightarrow \Delta(\Omega)$ . It means that  $\mathcal{P}_i$  is the sets  $\{\mu \in \Delta(\Omega) : \mu(E) \geq \alpha\}$  for all  $E \in \sigma_i(w)$  and rational number  $\alpha \in [0, 1]$ .

Thus we extend the  $G$ -frame to  $F_G = \langle \Omega, \{\mathcal{K}_i\}_{i \in N}, \{\sigma_i\}_{i \in N}, \{\mathcal{P}_i\}_{i \in N} \rangle$ .  $G$ -model is also extended by adding to  $F_G$  the following valuation:

- $w \models \mathbf{i}_{m\theta_{n_i}}$  if and only if  $\sigma_i(w) = \mathbf{i}_{m\theta_{n_i}}$ , and  $\mu_i(\sigma_i(w)) = \theta_{n_i}$ .
- $w \models \mathbf{u}_i(1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}) = \mathbf{r}_{i, 1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}}$  if and only if  $u(\sigma_i(w), \sigma_{-i}(w)) = r$  and  $\mu_{i,w}(\sigma_i(w), \sigma_{-i}(w)) = \theta_{n_i, n(-i)}$ .
- $w \models \mathbf{P}_i(\varphi) \geq b$  if and only if  $\mu_{i,w}(\sigma_i(w), \varphi) \geq b$  while  $\sigma_{i,w}(\varphi) = \{w \in \sigma_{i,w} | w \models \varphi\}$ .

The proposition that captures the rationality of player  $i$  with type  $\theta_{n_i}$  is called **rattype<sub>i</sub>**. The axiom **RATType** which is the formalism of utility maximization by considering a player's type is defined as the following equivalence:

$$\begin{aligned} \mathbf{rattype}_i &\leftrightarrow \bigwedge_{m \in \Theta_i} \left( (K_i \bigwedge_{1_{k_1}, \dots, N_{k_N}} \sum_{1_{k_1}, \dots, N_{k_N}} \mathbf{P}_i(\theta_{n_i, n(-i)}) \right. \\ &\quad \left. \mathbf{u}_i(1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}) = \right. \\ &\quad \left. \mathbf{r}_{i, 1_{k_1}, \dots, N_{k_N}, \theta_{n_i}, \theta_{n(-i)}} \wedge \mathbf{i}_{m\theta_{n_i}} \right) \rightarrow \\ &\quad \bigwedge_{1_{k_i}} \sum_m \mathbf{P}_{m\theta_{n_i}} \cdot \mathbf{r}_{i, 1_{k_1}, \dots, i_m, \dots, N_{k_N}, \theta_{n_i}, n(-i)} \\ &\quad \geq \sum_{1_{k_i}} \mathbf{P}_{1_{k_1}\theta_{n_i}} \cdot \mathbf{r}_{i, 1_{k_1}, \dots, i_i, \dots, N_{k_N}, \theta_{n_i}, n(-i)} \end{aligned} \quad (1)$$

The above axiom states that player  $i$  is a utility maximizer whenever, if he decides to play his  $m_{\theta_i}$ th strategy in a situation in which he has probabilistic beliefs  $\mathbf{P}_i(\theta_{n_i}, n(-i))$  about utility (captured by the  $\mathbf{r}_{i, k, l, \theta_{n_i}, \theta_{n(-i)}}$ ) then the  $m_{\theta_i}$ th strategy is better than any other, given his beliefs.

At this stage the valuation function for  $G$ -model satisfies the following extra condition:

- $w \models \mathbf{rattype}_i$  if and only if, for every  $s_{i\theta_{n_i}} \in S_i$  there exists an  $w' \in \mathcal{K}_i(w)$  such that  $u(\mathbf{i}_{m\theta_{n_i}}, \sigma_{-i}(w')) \succeq u(s_i, \sigma_{-i}(w'))$  and  $\mu_{i,w}(\sigma_i(w), \sigma_{-i}(w)) = \theta_{n_i, n(-i)}$ .

**Proposition 1:** The proposed epistemic logic is sound with respect to the class of  $G$ -models.

*Proof*

- Axioms **G'1** and **G'2** are valid in every model because at each state  $w$  there is a unique strategy  $\mathbf{i}_{m\theta_{n_i}} \in S_i$  such that  $\sigma_i(w) = \mathbf{i}_{m\theta_{n_i}}$ , and  $\mu_i(\sigma_i(w)) = \theta_{n_i}$  by validation rule  $w \models \mathbf{i}_{m\theta_{n_i}}$ , if and only if  $\sigma_i(w) = \mathbf{i}_{m\theta_{n_i}}$ , and  $\mu_i(\sigma_i(w)) = \theta_{n_i}$ .
- Axiom **G'3** because if  $w' \in \mathcal{K}_i(w)$  then  $\sigma_i(w) = \sigma_i(w')$  and by using  $\mu_i$  we have  $\mu_i(\sigma_i(w')) = \mu_i(\sigma_i(w)) = \theta_{n_i}$ .
- Axiom **G'4** is valid because if  $w' \in \mathcal{K}_i(w)$  then  $\sigma_i(w') = \sigma_i(w)$  and then we have  $u(\sigma_i(w), \sigma_{-i}(w)) = u(\sigma_i(w'), \sigma_{-i}(w))$  also by applying  $\mu_i$  we have  $\mu_i(\sigma_i(w')) = \mu_i(\sigma_i(w)) = \theta_{n_i}$  and because each  $\sigma_{-i}(w)$  is unique and has unique type  $\theta_{n(-i)}$   $\mu_{i,w}(\sigma_i(w'), \sigma_{-i}(w)) = \theta_{n_i, n(-i)}$ .
- Axiom **G'5** is valid because for every state  $w$  there is a unique profile strategies  $\sigma_{-i}(w)$  of the player other than  $i$  and the ordering of  $u_i(1_{k_1}, \dots, N_{k_N})$  induces an ordering of  $\bigwedge_m u(i_m, \sigma_{-i}(w))$  and also because each  $\sigma_{-i}(w)$  is unique and has unique type  $\theta_{n(-i)}$   $\mu_{i,w}(\sigma_i(w), \sigma_{-i}(w)) = \theta_{n_i, n(-i)}$  is unique and it does not have any effect on the ordering.
- **rattype<sub>i</sub>** is valid. The proof is same as using reasons for **G'1** till **G'5**. Besides we should deal with  $\mathbf{P}_i(\theta_{n_i, n(-i)})$  and with respect to third valuation function it is straight forward.

		Node j $\theta_j = 0$			
		Monitor		Idle	
Node i $\theta_i = 1$	Attack	$-u_A - c_A$	$-u_A - u_M$	$u_A - c_A$	$-u_A$
	Cooperate	$-u_C$	$-u_M$	$-u_C$	0
		Node j $\theta_j = 0$			
		Mintor		Idle	
Node i $\theta_i = 0$	Cooperate	$-u_C$	$-u_M$	$-u_C$	0

TABLE I  
PAYOFF MATRIX OF AN ATTACKER DETECTION GAME [5]

### III. BAYESIAN ATTACKER DETECTION GAME

Attacker detection games are proposed by Wang et al [5]. In this section we summarize this game and its analysis.

**Attacker detection game [5].** These games model the interaction between the potential attacker node  $i$  and the regular node  $j$ . The regular node cannot tell if node  $i$  is an attacker or not, instead it can only detect the attacker through observations. Nodes can have different types, and these types are their private information.

Here as the game has two nodes (players), we have two types namely  $\theta_i$  for node  $i$  and  $\theta_j$  for node  $j$ . While  $\theta_j = 0$ , i.e., always regular,  $\theta_i$  can be either 1 (attacker) or 0 (regular), depending on its true type. This game is a Bayesian game as the type of node  $i$  is hidden, and the observation is not accurate due to noise. The strategies  $s_i$  of node  $i$  are based on its type. For  $\theta_i = 0$ ,  $s_i = \{\text{Cooperate}\}$  that is, the only strategy available to a regular node is cooperation. For  $\theta_i = 1$ ,  $s_i = \{\text{Attack}, \text{Cooperate}\}$ , i.e., an attacker can camouflage as regular. Node  $j$

		Node j			
		Monitor		Idle	
Node i	attack, cooperate	$p(-u_A - c_A) + (1-p)(-u_C)$	$p(u_A - u_M) + (1-p)(-u_M)$	$p(u_A - c_A) + (1-p)(-u_C)$	$p(-u_A)$
	cooperate, cooperate	$-u_C$	$-u_M$	$-u_C$	0

TABLE II  
THE INDUCED NORMAL FORM OF BAYESIAN ATTACKER DETECTION GAMES

has the option to monitor or be idle regardless of whether node  $i$  is attacking or not, thus node  $j$  has two available strategies  $s_j = \{\text{Monitor, Idle}\}$ . Because the scenario is modeled based on the game theory approach we need a payoff matrix. For this purpose the following values are assumed.  $u_A$  is considered as the payoff of an attacker node if it successfully attacks. The cost associated with such an attack is  $c_A$ . The cost of monitoring is  $u_M$  for the regular node  $j$  and 0 if it is idle. Therefore, for the strategy profile  $(s_i, s_j) = (\text{Attack, Idle})$ , the net utility for a successful attacker  $i$  is  $u_A - c_A$ , the loss for node  $j$  is  $-u_A$  due to the attack. Similarly, if the strategy profile is  $(s_i, s_j) = (\text{Attack, Monitor})$ , the attacker node  $i$  loses  $u_A + c_A$ , and the net gain for node  $j$  is  $u_A - u_M$ .

Nevertheless, if an attacker node chooses to cooperate, the cost is  $u_C$ . Based on the types of node  $i$  and node  $j$  and their strategies, the payoffs matrices are shown in table I. In this work we also assume that  $u_A > u_m > u_C > c_A$ .

In this game by monitoring both nodes develop knowledge about their opponent over time. Developing the knowledge is useful because it decreases the costs for both players. For the regular node, it is not optimum to monitor always due to the cost of monitoring. It is also not suitable for attacker node to attack all times because it increases the chance of detection. While node  $j$  is monitoring, it acquires a knowledge about node  $i$  on whether it is an attacker or not. This knowledge is updated over time whenever node  $i$  is observed to be an attacker. This observation is possible from the attacker node's point of view. Despite of the fact that the uncertainty of the wireless medium makes the observations inaccurate, the more often the attacker attacks, the quicker node  $j$  can develop knowledge about its attacker type. The strategies adopted by node  $i$  is only determined by the current state of the knowledge, i.e., when the knowledge update process takes place. However, the knowledge held by node  $j$  is its private information, and node  $i$  does not have access to this information. Thus, it is important for node  $i$  to develop its own knowledge system.

#### IV. REASONING BY EPISTEMIC LOGIC

Due to the uncertainty in Bayesian games, a Bayesian game is modeled as a set of games that differ only in their payoffs,

and a common prior defined over them. For Bayesian games the counterpart of the Nash equilibrium is called the Bayes-Nash equilibrium. This equilibrium for agent  $i$  is a mixed strategy profile which is the best response to a mixed strategy profile of the other player. The Bayes-Nash equilibrium may seem conceptually complicated. However, the solution is to construct a normal form representation that corresponds to a given Bayesian game. This representation is called an induced normal form. We now reason why we should transform the Bayesian games to their induced normal forms. The pattern of reasoning here is adopted from [12].

For the attacker detection games with two players, attacker and regular nodes, if the current state is a member of the equivalence states (the states that are connected by an accessibility relation in the Kripke models) that the attacker node currently considers as possible states, it also might consider many possibilities for what the equivalence states of the regular node might be. Thus, the attacker node must take into account what the regular node is likely to do in all of these circumstances. But regular nodes choice depends on the states it considers possible, and it may consider a state possible that is not in the actual equivalence states of the attacker node. And so on. We therefore have to take into account all reachable states, that is (because our model is connected) all states in the model. This means that the attacker node has to know what the regular node might do in any of the states in the model, independent from his (regular node) actual state, and similarly for the attacker node. This explains why strategies are formulated as contingencies for every state in the model, i.e., as functions from every state to a choice of strategies in that state. These strategies and their expected payoffs define normal induced games for Bayesian games as our case here the attacker detection games. Payoffs are computed by taking the average over all states in the model. It is clear that it does not suffice to look only in the current state, as each agent also might consider other states possible. But why not, then, compute a players payoff by taking the average over all the states that that agent considers possible, i.e., that agents equivalence class? We cannot, because the strategic game must be common knowledge, in order for solution concepts such as the Nash equilibrium to make sense.

Here for the game from table I we have two players and two games. To model the scenario based on the logic from II we consider the attacker node as **1** and the regular node as **2**. The players do not know which game is about to be played. Therefore we represent the game as an induced normal form game. The assumption is that  $\theta_i = 1 = \theta_1$  with probability  $p$  and  $\theta_i = 0 = \theta_0$  with probability  $1-p$ . 'co' is the abbreviation

of cooperate and 'att' is the abbreviation of attack. For the first normal game the logical notation for attacker node's strategy profile is  $(\mathbf{1}_{co}, \mathbf{1}_{att})$ . Note that in the Bayesian game the attacker node has three possible pure strategies. These pure strategies are derived from the two types and the two actions of the player. Then the attacker's three strategies in a Bayesian game can be labelled "the first action in first type" ( $att\theta_i = 1$ ) "the second action in first type" ( $co\theta_i = 1$ ) and "the second action in second type" ( $co\theta_i = 0$ ). The logical notations respectively are  $\mathbf{1}_{co\theta_1}$ ,  $\mathbf{1}_{att\theta_1}$  and  $\mathbf{1}_{co\theta_0}$ .

The regular node has only one type and two pure strategies  $\mathbf{2}_{monitor}$  and  $\mathbf{2}_{idle}$ . Now we have a  $2 \times 2$  normal form game in which the utilities are the ex-ante expected utilities in the individual games, given the agents' common prior belief. The ex-ante utility is an expected utility in which players know nothing about the other players actual type. The payoff matrix for this attacker detection game is constructed which is the induced normal form of this game. It is given in table II.

As we assume that  $u_A > u_m > u_C > c_A$  we have  $u_A - c_A > u_A - u_M > 0 > -u_C > -u_M > -u_A > -u_A - c_A$ . We now specify the axioms for the attacker detection game:

- $\mathbf{1}_{co\theta_1} \vee \mathbf{1}_{att\theta_1} \vee \mathbf{1}_{co\theta_0}$
- $\mathbf{2}_{monitor} \vee \mathbf{2}_{idle}$

The above formulae mean that each node should choose one strategy at each state.

- $(\mathbf{1}_{co\theta_1} \rightarrow \neg(\mathbf{1}_{att\theta_1} \vee \mathbf{1}_{co\theta_0})) \wedge (\mathbf{1}_{att\theta_1} \rightarrow \neg(\mathbf{1}_{co\theta_1} \vee \mathbf{1}_{co\theta_0})) \wedge (\mathbf{1}_{co\theta_0} \rightarrow \neg(\mathbf{1}_{co\theta_1} \vee \mathbf{1}_{att\theta_1}))$
- $\neg(\mathbf{2}_{monitor} \wedge \mathbf{2}_{idle})$

These formulae say that each node can not choose more than one strategy at each state

- $K_1 \mathbf{1}_{co\theta_1} \leftrightarrow \mathbf{1}_{co\theta_1}$

It says that attacker node knows his own strategies which here is cooperation with type  $\theta_1$ .

- $u_1(\mathbf{1}_{co}, \mathbf{2}_{monitor}, \theta_1) = -u_A - c_A \rightarrow$   
 $K_1 u_1(\mathbf{1}_{co}, \mathbf{2}_{monitor}, \theta_1) = -u_A - c_A$

It says that attacker node knows its own utility at this state.

- $\mathbf{r}_{1,1co,2monitor,\theta_1} \succeq \mathbf{r}_{1,1att,2monitor,\theta_1}$

It shows that the ordering of strategies are complete.

- $\mathbf{ratttype}_1 \leftrightarrow K_1((\mathbf{P}_1(\theta_1)\mathbf{u}_1(\mathbf{1}_{att}, \mathbf{2}_{monitor}) \wedge \mathbf{P}_1(\theta_0)\mathbf{u}_1(\mathbf{1}_{co}, \mathbf{2}_{monitor})) = \mathbf{r}_{1,1att,1co,2monitor,\theta_1,\theta_0} \wedge (\mathbf{P}_1(\theta_1)\mathbf{u}_1(\mathbf{1}_{co}, \mathbf{2}_{monitor}) \wedge \mathbf{P}_1(\theta_0)\mathbf{u}_1(\mathbf{1}_{co}, \mathbf{2}_{monitor})) = \mathbf{r}_{1,1co,1co,2monitor,\theta_1,\theta_0} \wedge (\mathbf{1}_{co\theta_1} \wedge \mathbf{1}_{co\theta_0})) \rightarrow \mathbf{P}_{1co\theta_1} \wedge \mathbf{P}_{1co\theta_0} \mathbf{r}_{1,1co,1co,2monitor,\theta_1,\theta_0} \geq \mathbf{P}_{1att\theta_1} \wedge \mathbf{P}_{1co\theta_0} \mathbf{r}_{1,1att,1co,2monitor,\theta_1,\theta_0}$

The above axiom states that player 1 is a utility maximizer whenever, if he decides to play his  $(\mathbf{1}_{co\theta_1} \wedge \mathbf{1}_{co\theta_0})$  or  $(\mathbf{1}_{att\theta_1} \wedge \mathbf{1}_{co\theta_0})$  strategy in a situation in which he has probabilistic beliefs  $\mathbf{P}_1(\theta_1) \wedge \mathbf{P}_1(\theta_0)$  about utility then the  $(\mathbf{1}_{co\theta_1} \wedge \mathbf{1}_{co\theta_0})$  strategy is better than the other, given his beliefs. This pattern is reasoning can be continued to find the best response for both nodes. The result is the Bayes-Nash equilibrium.

Now we can have an axiom for detection of attack.

- $\mathbf{detect\_attack} \leftrightarrow K_2(\mathbf{P}_1(\theta_0)\mathbf{1}_{co\theta_0}) \wedge \mathbf{P}_1(\theta_1)\mathbf{1}_{att\theta_1} \wedge \neg\mathbf{2}_{idle}$

says that the regular node can detect the attacker node when it develops knowledge about strategies and forms a probabilistic belief about the performance of the attacker node and when it is not idle. The axiom is correct because the regular node develops the knowledge about the strategies of the attacker node and its types which means that in any state that the regular node considers possible and by the accessibility relation is related to equivalence states if at those states its strategy is not idle, the regular node can detect attack.

In this section we have transformed the Bayesian attacker detection games into the induced normal form then and we model the game based on the epistemic logic developed in section II. We show that if the nodes are rational they try to maximize their own utilities. And also we show that in which state the regular node can detect the attacker.

## V. CONCLUSION

Because of an increasing number of applications of wireless networks with collaborative nodes, the security of these networks has been receiving increasing attention among researchers in recent years. However, little has been done so far in terms of the definition of security needs specific to different types of scenarios that can be defined for wireless networks. One approach is to model attacker detection with uncertainty of node types as a Bayesian game in the game theoretic scenario.

However the conceptual study of Bayesian game-playing situations cannot be used to derive stable results as long as no appropriate formalism is available to model the situation. The main purpose of this paper was to show that a formal tool, namely epistemic logic for normal form games can be used to represent and reason about Bayesian games. However, special propositions and axioms are introduced to model the uncertainty of players about payoffs in Bayesian games. We show that this language provides reasoning about the Bayes-Nash equilibrium in Bayesian games. By using the language for representing and reasoning about Bayesian attacker detection games, an example application of this language is provided. Although we show the use of the extended language to verify some specifications of Bayesian games such as the solution concept, these verifications for these games can also be performed through model checking. In general, model checking allows us to test whether a defined model or system meets a given specification. The inputs into a model checker are the description of a system to be analyzed and a number of properties, often expressed as formulae of one kind of logic. In the future, we plan to develop a model checker that supports the epistemic logic for Bayesian games.

## REFERENCES

- [1] C. Westphal, "A study of the percolation threshold for k-collaborative wireless networks," in *Communications, 2009. ICC '09. IEEE International Conference on*, june 2009, pp. 1–6.
- [2] S. Song, D. Goeckel, and D. Towsley, "Collaboration improves the connectivity of wireless networks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, april 2006, pp. 1–11.

- [3] H. Ochiai, P. Mitran, H. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *Signal Processing, IEEE Transactions on*, vol. 53, no. 11, pp. 4110 – 4124, nov. 2005.
- [4] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation," in *Mobile Ad Hoc Networks, Communication and Multimedia Security*, 2002.
- [5] W. Wang, M. Chatterjee, and K. Kwiat, "Attacker detection game in wireless networks with channel uncertainty," in *Communications (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –5.
- [6] J. R. Galliers, "A theoretical framework for computer models of cooperative dialogue, acknowledging multiagent conflict," Ph.D. dissertation, Open University (United Kingdom), 1988, aAIDX87541.
- [7] A. Jøsang, "Probabilistic logic under uncertainty," in *Proceedings of the thirteenth Australasian symposium on Theory of computing - Volume 65*, ser. CATS '07. Darlinghurst, Australia, Australia: Australian Computer Society, Inc., 2007, pp. 101–110. [Online]. Available: <http://portal.acm.org/citation.cfm?id=1273694.1273707>
- [8] G. Bonanno, "A syntactic approach to rationality in games with ordinal payoffs," in *Logic and the Foundations of Game and Decision Theory*, ser. LOFT 7, G. Bonanno, W. van der Hoek, and M. Wooldridge, Eds. Amsterdam University Press, 2008, pp. 59–86.
- [9] B. de Bruin, *Explaining Games: The Epistemic Programme in Game Theory*, ser. Synthese Library. Springer, 2010. [Online]. Available: <http://books.google.com.au/books?id=G1-c0uZEOcYC>
- [10] R. Fagin and J. Y. Halpern, "Reasoning about knowledge and probability," *J. ACM*, vol. 41, no. 2, pp. 340–367, Mar. 1994. [Online]. Available: <http://doi.acm.org/10.1145/174652.174658>
- [11] P. Halmos, *Measure Theory*, ser. Graduate Texts in Mathematics. Springer, 1974. [Online]. Available: <http://books.google.com.au/books?id=-Rz7q4jixUC>
- [12] T. Ågotnes and H. P. van Ditmarsch, "What will they say? - public announcement games," *Synthese*, vol. 179, no. Supplement-1, pp. 57–85, 2011.