JOURNAL OF MEDIA AND INFORMATION WARFARE

VOLUME 5 · JULY 2014 · ISSN 1675-1302

اونيۏرسيتي تيكنولوݢي مارا
UNIVERSITI
TEKNOLOGI
MARA

CMIWS
Centre for Media and Information Warfare Studies
Universiti Teknologi MARA

The views, opinions and technical recommendations expressed by the contributors and authors are entirely their own and do not necessarily reflect the views of the editors, the publisher and the university.

JOURNAL OF MEDIA AND INFORMATION WARFARE

VOLUME 5 · JULY 2014 · ISSN 1675-1302

Towards A New Model for Information Warfare

Abdulrahman R. Alazmi

Kuwait University, Libraries Systems and Technologies – Libraries
Administration, Khalidiyah, Kuwait

abdulrahmanr.alazmi@ku.edu.kw

Abstract

In the current information-rich environment, it has become routine to broadcast and receive information via the media and most importantly the Internet. And with such flexibility in the distribution of information and its channels comes the huge risk of the information being compromised, tampered with, or corrupted. Such intentional acts of compromising and corrupting information for a certain goal constitute what is known as Information Warfare. Because Information Warfare can be carried out on different forms of communication and channels in information flows, devising a model to simulate the attacks is vital to analyse and prevent information tampering. Many models have been proposed that use an array of underlying theories that range from schematic modelling, to information science and cognitive studies. However, the problem is that modelling the Information Warfare battle theatre using existing models

ISSN 1675-1302

results in tabular and tree schemas that are populated by percentages and numbers, which reflect the information attack but in a difficult and non-visualized manner. In this paper, attempts will be made to introduce a new modelling scheme to capture the elements of Information Warfare, including the participating parties, attacks, channels, and noise in the form of models that use information flow and visible entities. Because Information Warfare can have many forms, and can be made at several levels, several existing models lack some design elements that are critical in capturing the attacks. The model developed here will investigate, precisely, the information exchanged between the entities and their state. Information exchange can show where information is from and where it is destined to go, while, entity states provide what type of information is flowing. The methods of the modelling proposed in this paper incorporate several established modelling methods that include Information Flow Model and Game Theory, and forms of asynchronous communication.

Keywords: *asynchronous communication, flow model, game theory, information warfare*

1.0 Introduction

The telecommunication networks, satellite networks, the Internet, and the mass media all overlay our knowledge sphere, willingly or unwillingly, to the point where we can no longer determine the information we receive, its source, its authenticity, or its state, whether this information is quoted, original, or corrupted. And with the wealth of data spread around the Internet – one of the contemporary silos of our knowledge – it becomes even more difficult to differentiate data from information. Data are numbers, figures, and letters, while information is a collection of data where a conclusion or a fact can be extracted. Knowledge, however, is the state where information can be predicted, analysed, understood, and connected. Not being able to connect, understand, or authenticate the information source, validity, or completeness becomes a major threat in information systems, databases, and strategic and military situations.

Since information is all around us, and its channels are mostly open and unsecure, the quality of information we receive and its integrity should be questionable, at least if we are talking about vital and sensitive information, with which an enemy can gain an advantage from its misuse, information that can compromise individuals, and organizations. This type of information is the typical target for Information Warfare campaigns. Information Warfare (IW) can be defined as the usage of information to gain an advantage over an opponent. This can be achieved by tampering with the information, corrupting its data, reading its sensitive content, disabling it, or concatenating it with additional data. In light of this definition, we can consider IW no less important than any other type of warfare and, as in any warfare, strategy and modelling of the situations and attacks are keys to gaining advantages. As with any warfare campaigns, the attackers can initiate their attacks at different levels, with varied forms of attacks, and employ a wide range of tools and techniques.

The primary use of IW is in the military battle theatre, but it is not to be confused with the more general term of Command and Control, as stated in [1], where IW is used as a tool. IW encompasses many elements including information exchange protocols, human communication theories, political correctness of practices, game theories, and the public domain range of information. IW plays a key role in the military field; its strategies and tools are studied as part of military disciplinary curriculum.

In this paper, attempts to make a new modelling scheme in order to capture IW battle theatre will use the Flow Model (FM), which was founded by [2], because it will help in formulating a model for an IW battle theatre by enabling more granular description of information flow, with its representation of states. FM models the state of information in one entity and the flow of information from state to state and from entity to entity, and a single entity can have several states, and several flows of information. Identifying the state of the information and its source and destination is integral in developing a strategy for IW, and FM provides the necessary tools. The FM provides a way to identify the roles of the communicating parties whether actively creating, transferring, and processing information, or passively, as in receiving and releasing information. Entities can be asymmetrical and have different states; flow of information can occur inside the states of the same entity or from one entity's states to the states of other entities.

The second of the tools that will be used is the use of Game Theory in developing strategies for IW tactics, as used in [3], and examples will be given to illustrate the situation. Game theory provides analytical tools and algorithms that when used by a computer can help in predicting the enemy's next movement and suggest several possible courses of action that would follow the scenario at hand. Game theory also provides many forms that can be adapted to different situations (such as game type) and, with this flexibility, IW attacks can be modelled and solutions for them can be found or, at least, IW battle theatre situations can be modelled.

The paper is organized as follows: in Section II related work in the field of information, IW, modelling, and FM modelling and game theory modelling will be discussed. In Section III, game theory is described, and how a game theoretic approach can yield grounds for modelling IW battle theatre attacks is explained. Section IV illustrates further examples and models of game theory using examples from IW, with asynchronous communication and hyper games. Both asynchronous communication and hyper games are realistic models of IW attacks. In Section V, the extended FM will be shown, in which FM is extended to include asynchronous communication, and is called FM Extended (FME). Section VI includes a case study in which the implementation of an example, its modelling, and the amalgam model (FM + FME + Game Model) will be used in a very well known puzzle game based on the absence of knowledge (asynchronous communication). Section VII contains a discussion of the results of the models made in the figures and the case study example in Section VI, and assesses how the models have helped in viewing the solution for the example. Finally, section VIII contains concluding remarks.

2.0 Related Works

The field of information warfare has attracted the attention of many researchers from the communication field, because IW is almost always defined in communication terms, as many researchers view it from this perspective. The United States Air Force (USAF) defines IW as ‘activities taken to manipulate or destroy an adversary’s information without visibly changing the physical entity within which it resides’ [4]. From the works of [5], we can define IW as ‘any action to deny, exploit, corrupt or destroy the enemy’s information and its functions; protecting ourselves against those actions and exploiting our own military information functions’. These four main strategies have been the basis of IW studies by [6]. The first is to deny; it is the act of denying the receiver access to information at the source, which is also in [7]. The second strategy is to exploit; this is the act of knowing the information passed and utilizing it to one’s advantage. The third strategy is to corrupt; this is the act of changing or altering the information from the source, in order to use that to our advantage. The fourth and last strategy is to destroy; this is the act of overwhelming the information with enough noise such that it is useless at the receiver’s end, as if had been destroyed. IW can also be a tool to prevent military actions. While not a diplomatic action, engaging in careful IW can still prevent wars and make way for a non-aggressive, yet transgressive attitude that abhors military action, and clever IW can solve, or soften situations, as stated in [1] . Understanding IW also implies a knowledge of information theory, and human intelligence: how humans think and upon what bases they act. In [1], it is stated that forming a hierarchy is critical, such as in Decision Support Systems (DSS), and Management Information Systems MIS. The Command and Control (C2), and the Observe, Orient, Decide, and Act (OODA) paradigm are both paradigms used to analyse decision making activities and affecting factors in the decision making process. These form cognitive hierarchies.

For the modelling of IW, the early works and one of the most fundamental is as in [8]. In his model Shannon defines IW as the capacity of the channel between a sender and receiver as C, where we have the bandwidth W, and signal vs. noise power P/N, given by this equation:

$$C = W \, Log\, 2\, (1 + P/N) \qquad (1) \qquad \textit{from Shannon (1948) [8]}$$

Shannon's work, although it has been the basis of many works such as those of [5] and [9], lacks the state of the information when it is being transferred such as released, created or processed, which is noted by the [10]. As described in [2], where the foundation of the Flow Model is found, the FM model defines the five states of information (created, released, received, processed, and transferred); furthermore, it also defines the flow of information from one state to another, or from one entity to another. The FM is used to model Open Systems Interconnection (OSI) layers; it is also compared to Shannon's communication model. In relation to things that flow, the (OSI) model makes it possible to have a more granular view of each layer in the OSI. Using the FM to model IW strategies should provide more information since previous work, such as Shannon, has ignored the information states. The idea of states in the FM is essential in its usage, since it gives greater elaboration to the modelled system.

In the works of [3] and [11], Game Theory is used as a tool to model IW strategies. A Game Model (GM) can model many real-life situations if we can identify the system we want to model as a game, where we have players, goals, and conditions. GM provides means to predict, or anticipate the attacker moves by using the correct algorithms for determining the Course of Action (COA), given a correct GM model that would model the exact IW theatre. In addition, GM provides the means to suggest better COAs to prevent attacks from the enemies by analysing the possible scenarios of the current situation. However, as pointed out by [3], using heuristic algorithms may either take time to processes, or may result in non-optimum solutions, and may hinder the potential of using game theoretic approaches to IW. Moreover, game theory itself is difficult to implement in the dynamic field of IW. The bases for modelling using GM are two elements which form the tactical engine; they are the search technique, and the evaluation function. The first determines what is the most advantageous move to take, while the second element evaluates the players' positions and how vulnerable each one is, and what the advantages are for each player's position. Therefore, initiating the search technique (which is mostly a heuristic algorithm) will produce several actions by the players, and their consequences, and so form a tree. After that, the evaluation function will gather the weights of value on each level of the tree, and produce the best COA for the player.

[12] explains just how important IW is, and how much economic impact it has. Burke also shows how IW is still not well understood, despite its importance, by some governments and institutions because of its complexity and interoperability with other disciplines. IW is complex because of its varied elements and conditions; for example, the attackers can have many different goals and objectives; the attackers also have many subtle and unorthodox ways of approaching their targets. He suggests the use of the Game Theory approach to help formulate and model the IW battle theatre. Burke suggests the use of the Game Theory approach to help formulate and model the IW battle theatre. The reason behind this is that game theory has proved itself in the diplomatic and military fields. However, game theory application and modelling is challenging by itself. Incorporating game theory elements (which include: players, goals, strategies, equilibrium, and repeated games - with absence of knowledge), Burke modelled an IW situation as a repeated game (with absence of knowledge and predicting strategies). Problems arose from the fact that game and IW principles collided, and it was difficult to find a middle ground. For example, in the experiment the players were randomly chosen types, and it was assumed that different types did not affect the overall equilibrium calculations. This, however, is a compromise made for the sake of illustrating the concept. In the end, the findings in [12] showed how critical it is to model IW, and how appropriate Game Theory is to model IW. In his work, Burke described the IW Game theoretic model as basic elements which are: the players, payoff, information, and moves. The second level is the game representation model, whether normal form or extensive form; and the third level is the equilibrium, whether Nash Equilibrium or Bayesian Equilibrium. The final level is the repeated games that incorporate absence

of knowledge. Developing these levels, from one to four, the modeller must improve in building this model to ensure a detailed and well-planned model that has the potential to be used in real-life military situations, which need formal modelling schemas that are reliable and trustworthy. Software can also be used after careful modelling of the IW battle theatre.

IW has seen many adaptations, most prominently using Game Theory. The only drawbacks that have been seen are the difficulties in implementation and the complexity of GM algorithms themselves. The modelling used range from simple tree structure to simple UML like charts. These modelling schemas lack high level details, and information state and information flow as well. Developing a modelling schema to model GM and IW attacks is critical in solving this problem.

FM has been introduced in Sabah [2] and it has been used in many fields that include, but are not exclusive to, its proposed application in database access control [13] and in information security [14]. FM is based on two main ideas: flow-things, and information states. The first is the idea that information (or any signal, wave, or any communication channel) can travel from one entity to another. The second is that entities can have many states and information travels from state to state; information can travel from states of the same entity or to a different entity's states. There are six basic states which are: released, transfer, processed, created, arrived, and accepted. The first is when the flow-thing is released from one state to another; 'transfer' is when a flow-thing is being transferred from one state to another; 'processed' is when a flow-thing is being updated or modified; 'created' is when a flow-thing is being originally created at the entity; 'arrived' is when a flow-thing is being received from another state or another entity's state; and 'accepted' is when an entity has accepted the flow-things. There is a seventh state, which is 'storage', but this is not standard to FM, and it is only used when needed; it indicates when an entity stores flow-things, leaving FM with its default five states and the standard flow between them, as shown in Fig. 1. It is worth noting that FM is very flexible; any modeller can use any number of states to model the entity and even the default information flow can be changed as well to accurately model the entity [15] . FM will provide a visual representation to IW when used to model IW battle theatre. This will be used in this paper in addition to GM, and with a modification to FM that is novel to this paper.

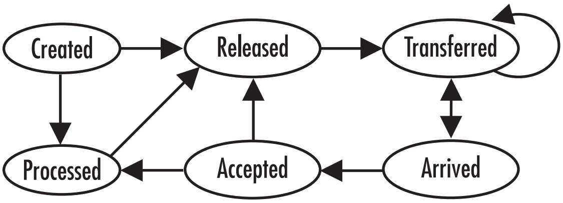

Figure 1: The FM model

Most modelling methods used to model IW consider synchrony in communication or disregard the element of time in communication through negligence of its effect; however, this leads to gaps in these models, such as the normal and extensive game models. Asynchronous communication can provide absence of knowledge, which of itself is a vital key element in IW. By introducing the time axis to the communication model we can have time stamped messaging between the entities; the use of logical clocks, in which each entity keeps track of its own time can also be used [16], but this will not be considered. In [17], asynchrony is modelled using vector clocks; again, they will not be considered. Adding time to the FM model will yield the FM extended (FME) model. FME will be explained thoroughly in Section V, and it is novel to this paper.

This paper shall demonstrate the modelling of an IW battle theatre in four different contexts: in the modelling FM, the extended FM (FM with asynchronous communication), GM, and a combination model (amalgam model) of all techniques (FM, FME, and GM). The asynchronous systems are introduced in order to develop more realistic situations, and to develop complex examples, extending the works of [3] and [12].

3.0 A Game Theory Approach

Game Theory provides not only models but also a strategic point of view with possible scenarios involving what each player would do to succeed. When modelling the IW battle theatre as a game, it is possible to model the attacks as games (e.g.: zero sums, constant sum, or non zero sum), in which we have players, goals, actions, and conditions. The COA can be predicted, depending on the game, attacks, as well as the motivation and alternative actions [3]. Game Theory has been used to model several concepts as games in many fields, including economics, biology, politics, and even philosophy. So Game Theory provides rich sets of mathematical tools that can be harnessed to model IW. An important and elemental principle in Game Theory is the Nash Equilibrium, which is the configuration for the existence of a win-win strategy in a game given the scenario and environment. This is a critical tool of analysis as its existence can change the inputs and output of the warfare, stemming from the strategy that provides the Nash equilibrium [12]. An example will be given in the following paragraphs to illustrate the models, and FM will also be used. The example will show the contrast in modelling IW in contrast to Shannon's model as set out in [8].

As an example, the example provided in [3], which is an excellent example of a Game Theory approach toward IW, will be studied in this section, and FM will be added to it. Figure 2 shows the example model. A brief summary of the example is: a Centralized Defence Controller (CDC) which defends the database A,B,C and D. The Internet, which is where the enemies reside, will probably launch an attack on CDC's database. CDC predicts that the attacks will come from the firewall's weakest link, and then tries to fishbowl the

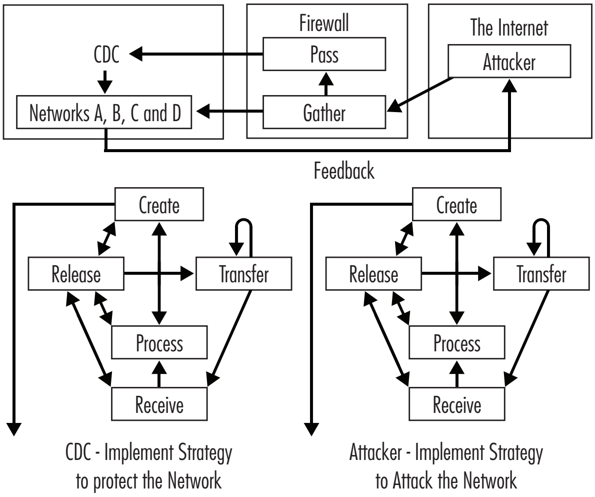

Figure 2: FM Information Warfare Theatre

attacker and gives it false data to try to understand the attacker's intentions. In addition, CDC will try to replicate the database to increase availability in the case of a denial of service attack. After this we can see that CDC can predict the attackers' next move or at least take precautionary actions.

In Figure 2, the additions are the introduction of FM into the model. CDC flows of actions are modelled precisely because of information flow from external actions (from both the environment and the attackers). Understanding the triggers that cause such reactions from both the attacker and defender can make developing a protective strategy by the defender easier. Furthermore, the model now gives more insight to all entities. Using FM terminology of information exchange, we can see how the flow changes actions. While Shannon's Model lacks a state for information and focuses on the channels' capacity and clarity (Noise), by introducing FM we can capture the information's state, its influence and the subsequent actions that follow. The model also shows that the firewall can also be split into two flow models: one for the passing of users, while the other represents the information gathering mechanism, the information from which is later analysed by the CDC. The Internet has the expected "Enemy Attacker", which is also represented by a flow model. Finally the networks A, B, C, and D are also flow models along with the CDC itself. When a suspicious activity is found at the firewalls this triggers an action of information being made at the CDC. Now CDC sends the made information to the network to suspect suspicious activity. Using this simple triggering mechanism the modeller can have a system that can anticipate attacks and can be used for analysis and scrutiny.

4.0 Hyper Games and FM

In the environment a flow of information may not always be visible to any party; in this case we have what is known as the absence of knowledge. [18] introduced the situation where information is not available, and we have to model the system as a hyper game. In a hyper game the participating players may:

- Not know the number of players
- Not know the choices available
- Not know the goal of the game

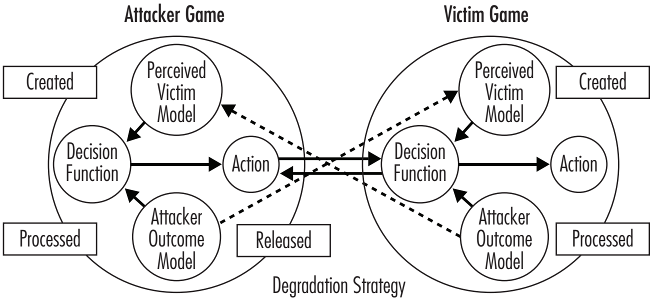

Figure 3: Hyper Games with FM notation

This is quite true in real life situations of IW, where deception, espionage, and undercover operations take place. So each player now has a perceived knowledge of the other players' strategies and moves, and based on that the player takes action. FM is introduced into the system in Figure 3. Figure 3 shows the introduction of FM elements into the model. As a complementary element, FM illustrates how and where information flows. For example, the player perceives information from the released or transferred information flowing from the other players and from their actions. Knowing the state of the information might give us a value of its authenticity and purpose, and allow the users to analyse the information more carefully [2].

An example is when the enemy – a competing player – tries to send deceptive information to lure the victim into performing certain actions; this can be prevented if the victim knew that the information was created by rather than released from the enemy. In light of this, the victim can develop strategies to prevent the four canonical attack strategies. As a last note, it can be seen that the models that have been introduced so far lack messages (information flow synchrony), the models do not show time flow and so the model viewer cannot know if the actions are casual, concurrent or sequential.

5.0 The Extended FM

So far the models that have been discussed did not deal with synchrony and assumed that the channels propagated the information synchronously. In the real world, information propagation is asynchronous between the parties,

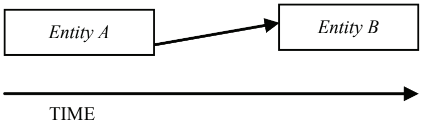

Figure 4: Time Variance

and to model this more accurately in the FM [15], extra elements need to be added. The dimension of time will be used to implement asynchrony, as in Figure 4. This is called the FM Extended (FME) and it is the proposed addition to the FM modelling schema, and is novel to the present work. FME captures information systems more realistically, as asynchronous systems are the prevailing types of systems, especially in communication. In a synchronous system the information flows from source to destination at the same time, while in an asynchronous system information arrives at the destination at a different time from when it was sent, and it can be delayed, lost, or out of order.

Using this notation, the model can show the viewer how fresh the information is (freshness means how much time has passed since this information was broadcast); since out of date information is either useless, or it may be delayed, this can reflect possible enemy intrusion. The FME extends the FM by introducing time, but synchrony is still difficult to model with one time axis. The model can also use logical clock [16], in which each entity keeps track of its own logical clock, while receiving the logical clock of the others when receiving information from them. A logical clock is a clock maintained by an entity to keep track of its own events. The need for logical clocks stems from the concurrency in the system and asynchrony; for example, maintaining physical clock synchronisation is impossible since actual physical clocks are never synchronous. Thus the use of logical clocks helps in synchrony, but a more robust approach would be to add Vector Clocks VC [17]. However, for simplicity VC will not be considered in the present case.

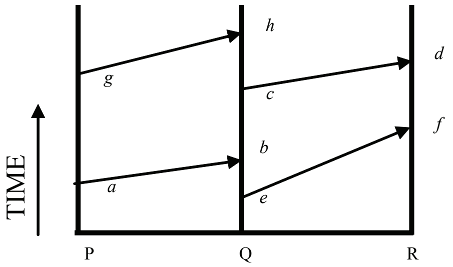

Figure 5: Concurrency (Source: Gosh, 2006)

In Figure 5, viewers can tell that (a) happened before (b), but cannot say anything about (g) and (f). In the case of (a) and (b), the viewer can have a partial order and so a form of causality, for (g) and (f) it can be said that they are concurrent, meaning there is no synchrony between them [17].

6.0 Case Study

In this section, an amalgam of Game Theory, FM, and the FME will be employed to model an example of an IW theatre. The model will include the information environment and its outcome on the players, environment, and the overall result of the system. The example that will be used is a classic example on IW, and the effect of knowledge in a system; it is also an example of how much absence of knowledge is as vital as its presence.

In the work of [19], the Cheating Husbands Dilemma (CHD) is presented. The paper presents the problem and gives variations for it. CHD shows how critical the flow of information is, whether direct or indirect, in an environment where one participant's movement can cause the participants to take actions based on that movement. In addition, the relation between information, actions and decisions is shown to be highly correlated. In relation to IW, the CHD dilemma can be considered as an example of an information attack. It also shows how absence of knowledge that is caused due to asynchronous communication can give rise to new actions in the entities' life time during the attack. FM will introduce flow of knowledge, GM will add the players and conditions for winning, while FME will introduce the time axis in terms of days and nights.

The Cheating Husbands Dilemma states:
"In a faraway land, the Queen has declared the following:
'There is at least one or more unfaithful husband in our land
Every wife who knows that her husband is unfaithful shall shoot him the night she discovers it
No wife knows anything about her husband, only the other husbands.
And a wife shall not exchange her information with other wives.'
Thus declares the queen."

In Figure 6, the FME flow model is used for the problem, which is an IW situation. The model captures each wife's information flow, and how a wife is influenced by the others' movements and actions. For simplicity, the problem will be solved under the assumption of one unfaithful husband. The new model which has been proposed shall provide helpful annotations that help in capturing the problem. FME highlights the time axis introduced, which is the day and night cycle. FM highlights the information flow, while GM gives the players and conditions. The model in Fig. 6 explains the problem thoroughly.

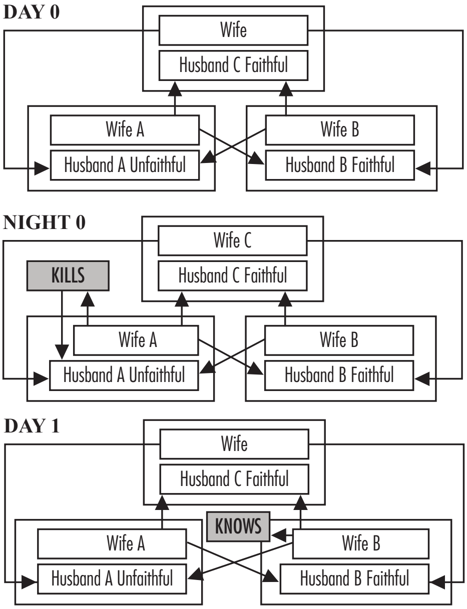

Figure 6: CHD modelled as a FME

	Wife A Shoots	**Wife A Does Not Shoot**
Wife B Shoots	*0/0* *Impossible*	*1/0* *Husband B IS Unfaithful*
Wife B Does Not Shoot	*0/1* *Husband A IS Unfaithful*	*1/1* *Impossible*

Figure 7: CHD modelled as a normal from game

Solution for One Unfaithful Husband: Let us assume that wife A's husband is unfaithful. Then all the other wives will know that since A's husband is unfaithful, the condition of "at least one unfaithful husband" is met, and they will not kill theirs. For wife A, since she hears no gun fire the first night, she knows that every husband besides hers is faithful. Again based on the first term of the Queen's declaration, wife A will deduce that her husband must be the unfaithful one to fulfil the term 1. So she will shoot him on the first night. The general solution is that if we had N unfaithful husbands, the wives will wait for N nights, and on the last night shoot their husbands.

Now in Figure 6 we can see that FME with GM portrays the solution. The Game Theory model alone, which can model the system using the normal form, might not show the flow of information nor the asynchrony involved which is shown in Figure 7, as in [17], in the case of a CHD with a population of two. We can embed each wife model in FME with the normal form as a base for the strategy of decision making. Indirect information flow is also shown as dotted lines, but nonetheless affects the participant players. We assume only three houses in the land, with families A, B and C. In DAY 0, it is the first day after the declaration, it can be seen that each wife is gathering information about the other wives' husbands. In NIGHT 0, in the night of the same day, each wife – without exchanging information - deduces facts from her gathered information. Wife A shoots her husband based on the information she got from her environment. The other wives hear gunshots and deduce that wife A has actually killed her husband. In DAY 1, each of wives B and C know for sure that the husband of Wife A is dead.

The CHD can be implemented in an information critical situation such as IW during combat, espionage, and/or conflict. The problem also introduces the idea of information deduction in case of the absence of knowledge (e.g. a wife cannot know about her husband's fidelity), and how critical the amount of information a player has, because too much information can also be harmful (e.g. if a wife did not know about all the other husbands, she will not shoot hers) [3, 12]. FME, FM, and GM in the amalgam model of Figure 6 have showed greater explanation for the problem solution.

7.0 Discussion

From the models introduced in Figure 3 and Figure 6, it can be seen that the model promulgated above has more clarity, which benefits its usage in IW. Because the main problems seen in existing IW models are that the models are rather difficult to understand, they come in tabular forms (as in Normal games), or as scenarios (as in Extended games). However, these often lead to numbers and figures scattered with no information flow or representations of entities, which is why FM and FME were added to GM and used together.

In Figure 2, using the FM, with GM, the IW situation can be seen. FM has modelled - each entity as a flow system, with flow-things moving states; the entities are the CDC, Firewall, and the Internet (where the attacker is). Flow of information from one entity to another can be seen, and from a certain state to a certain state. GM has introduced the players, which are the entities. It can be illustrated as a normal game using a tabular form. The granular view in Figure 2 shows CDC and the Internet, which is the attacker. Both have symmetrical schema, which shows that created information goes out directly, thereby representing new information, while received information can be processed and transferred, and this may indicate corrupt data. Received data, processed and released can also show data that has been tampered with. Since FM introduces information flow in the model, the designer has more capacity to convey more information. For example, if we had a larger environment with multiple attackers attacking at different layers and targeting different targets, the model would show its real capacity for capturing real life IW attacks. Also each entity can be modelled as an FM as well. Of course, this would increase the complexity of the model, but it would provide a finer and more granular view of the IW attack theatre.

From Figure 3, we see a Game Theory model of an IW battle theatre. FM elements were introduced into the model as well. The GM shows a Degradation Strategy in which outcome models affect the perceived opponent model. The perceived models have a state of Create, while the entity attack model has the Processed state. This is used because the entity attack model is used at every stage, and so it is processed, and might carry over from previous stages. On the other hand, the perceived opponent model creates information, because it is new or almost new at every stage, and so it is updated at every step. Both outcomes, processed and created, pour into the Decision Function, which can be a heuristic algorithm that is used as the search function from a game theoretic algorithm. Finally, the Decision Function will produce Actions that will go directly to the opponent. Figure 5 illustrated a hyper game in which each participating party has no knowledge of what the other players' goals are, the choices available, and/or the number of participating players in the game. FM and GM have helped explain the hyper game more clearly; if only words were used, and a more complex example was used, the explanation would not suffice. GM shows how each party flows from inception to decision of actions, while FM shows how each party's action affects the others, and how the internal information flow is in an entity. Indirect information flow is dotted, and it stems from the perceived model of attack from both sides. Viewers of the model can also notice that the created, processed, and released FM annotation shows the information and its state. This can help in analysing the data flow, its source and its credibility from both sides. For example, if the victim is receiving a piece of information that is created at the attacker, this should be handled with vigilance, as it is probably harmful in some form.

In Figure 4 and Figure 5 more elaborations are introduced to the models. The first shows information flow over the flow of time, since time was not considered earlier. This form of FM is called the proposed FME. FME can help in modelling asynchronous information flow. The latter figure, Figure 5, is the general form of a concurrent system, with several entities having asynchronous communication with one another (from [17]). Entities from a through are concurrent and are communicating; with the flow of time, it is critical to have a linear order for this communication in order to model the exact form of information flow. The simple UML, like the flow diagram in Figure 5, shows exactly at each point in time when and from whom each message is sent and received. Introducing such an element into a model for IW would be essential. In this paper, GM and FM have been used, and in Figure 6, FM, FME and GM are used together in order to incorporate all elements and properties that would capture a more detailed and complicated understanding of an IW battle theatre.

Moving on to Figure 6, where we have the CHD illustrated in FME and GM modelling schemas, we can see the whole CHD as a diagram or a flow chart. Because the example used a simple population of 3 entities (house A with Wife A, Husband A, house B, with Wife B, Husband B, and house C, with Wife C, and Husband C), it was easy to determine the data flow. However, this simplicity is adopted for time and space constraints, because a bigger population would at least double the size of this already large diagram. Yet again, using a more realistic number for the problem (e.g. more than 40), and modelling the problem using the FME and GM modelling proposed in this work, would prove very useful, and interesting in illustrating the solution, especially since its solution uses mathematics, but needs illustration to make it clear for scholars and readers. For example, with that number of population, trying to prove the general solution would be easier. The general solution, which states that if we had N husbands, the wives would take N nights to kill their own husband, from [19], will be modelled using the proposed model. Going back to Figure 6, we can see that we have the course of one day (DAY 0, NIGHT 0) and a half (DAY 1), and that is by following the logic of the puzzle. On DAY 0, we see that there is information flow as arrows show that, from FME, while GM provides that each house is an entity with two players, a husband and wife. Since the puzzle states that each wife knows about the fidelity and infidelity of each other wife's husband, but not that of her own husband, there is no information flow between a wife and her own husband. Moving on to NIGHT 0, since this example is also a hyper game, where there is an absence of knowledge, which is a critical and a real life aspect of most

IW battle theatre attacks, the players (active players, who are the wives) will act upon decided actions based on the absence of knowledge. Each wife would listen for a gun to fire, but since Wife B and Wife C already know that there is at least one cheating husband and it is husband A, they would not suspect their own husbands, even though they have no knowledge of his infidelities. Only one, who is Wife A, has the knowledge that both other husbands are faithful, so according to the rules of the puzzle that state there is at least one or more, she acts based on the absence of knowledge that hers is the one, and kills him; meanwhile, the other wives hear the gun fire. Again FME allowed the action KILL to flow from wife A to her husband, and again if we had a bigger population (simulated using software) the model would truly be useful. Finally, arriving at DAY 1, we have husband A dead, and the other wives would soon learn that, and the puzzle is complete. Wife A would also check on all surrounding spouses, but because the example used one cheating husband, the state of the system reaches equilibrium and its stays that way. The modelling could have used the GM in extensive form, which would lead to a tree, but again, since the actions of the puzzle follow one path (from root and down a single branch), its use was unnecessary. Fig. 6 showed FME in action, and it is simple to follow.

Finally in Fig. 7, the GM model for the CHD problem is shown. It is modelled as a normal game. All possible outcomes are mapped, but it lacks the landscape and granular view of FME. Since the puzzle has one solution, all other solutions are impossible except that wife A Shoots and wife B Does Not Shoot. Again GM hides many details and only shows the outcome. Its shows the players and conditions, but there are no representations of the information flow that took place in the problem. Furthermore, if the number of couples was greater than 40, the tabular form would be unreasonably large, and how information flow happened would be lost, with only the results shown.

8.0 Concluding Remarks

Information technology has made information ubiquitous, on more than any level we could have ever imagined in modern times, from radio, TV, media, Internet, and even in the palms of our own hands, with smart devices. It is almost impossible to ignore the flow of information, not just from trustworthy sources (e.g. books, official documents), but from almost any type of source (e.g. individuals, paid organizations, enemies who want an advantage, stalkers, or even a propaganda campaign from an organization or company). This relentless flow impacts all our information and knowledge spheres, and affects all levels of our interactions, and manipulates all fields of information, from news to databases (political and governmental issues aside). With that boon (or curse), information fidelity, integrity, and authenticity (especially in cases of sensitive information, information that can compromise individuals and nations as well), have become things of suspicion, because information channels are vulnerable and wide. Targeting information has become a feat of which many professionals and organizations are capable. If an enemy wanted to launch an attack using information (Information Warfare), then the enemy would go to lengths to make it as subtle as possible. To counter this requires a good modelling schema to model IW, and one which has the capacity to capture information flow.

A good basis for an IW model is a robust model to represent the information and the environment and, importantly, communication channels, information flow, and information states. Although several models to model the IW Theatre have been proposed, the majority ignore information states, and information flow. These modelling schemas give either tables or a collection of numbers to represent the IW, such as GM modelling or behavioural logs and statistics that indicate suspicious activities. This gap was the incentive for the present research; that is, to find alternatives to model IW, using FM, FM and GM, and a proposed FME.

In this paper, FM, GM, and and the proposed FME, as well as an amalgam model (which encompasses all three FM, FME, and GM) that incorporates the information states from FM, GM models and scenarios, have been used. The first introduces states and flow to the information representation elements and provides flow as to where the information is generated and where it will go, and the states of the information, whether original, created, or tampered with, processed, or in transition, released, or transferred. The second, which is Game Theory modelling, provides a tool to analyse the IW as a game model and then formulates strategies based on that abstraction and on well known algorithms, using a normal game model. The third and final addition, which is FME, is an extension to the FM that provides out-of-order communication, since FM assumes that all participants and users are in phase. This gives more realism to the modelling schema, and so enables modelling of a more complex and realistic problem, that is in need of illustration for proof and study purposes.

The amalgam model (of Figure 6) included GM, FM, and and the novel FME notations, where GM set the players, conditions, and enemy entities, FM introduced information flow, and entity and information states, and FME introduced the time and asynchronous communications. The model included players (wives and husbands), conditions (cheating husbands), information flow (knows, kills), and time and asynchronous communication (day 0, night 0, and asynchronous communication in information flow). The amalgam model still needs more thorough studies of its properties as well as a more rigid formulation connecting its main components (FM, GM, and FME) in one solid definition. These areas are subjects of further study. For example, the bonds between the separate models are still not very concrete, and the way the different elements of the different models interact still needs a more formal definitive way of application. Adding time to all the FM entities (which may or may not have all FM states), has been introduced by FME, but still needs more usage. In addition, using more game models to formulate the diagram (such as normal form, and extensive form), different Game Theory algorithms that predict enemy movements, can also be incorporated into an FME model, because we can model these elements using the time frames. Incorporating more modelling schemes into FME may also give it wider use. The amalgam model reached in this paper can also be adapted to model areas in information other than IW battle theatre. All these are areas for future study.

References

[1] V. Shalamanov, Journal of Information & Security, vol. 1 no. 2, pp. 59-66, 1998.

[2] S. Al-Fedaghi, Proceedings from ISSS ’08: *The 52nd Annual Meeting of the International Society for Systems Sciences.* USA, Madison: University of Wisconsin, 2008.

[3] S. Hamilton, et al. "The 4th Information Survivability Workshop" in Proc. *ISW* CERT Coordination Center, Software Engineering Institute, Vancouver, Abbrev. Canada, 2002.

[4] S. Widnall, and R. Fogelman, "Cornerstones of Information Warfare," Washington, DC: Department of the Air Force publication, 1997.

[5] A. Borden, (1999). *What is information warfare? Aerospace Power Chronicles.* United States Air Force, Air University, Maxwell Contributor's Corner. Available: http://www.airpower.maxwell.af.mil/airchronicles/cc/borden.html. Retrieved on September 11, 2011.

[6] D. Silverberg, "Interview with Vice Admiral Arthur Cebrowski, Director, Space, Information Warfare, Command and Control, Chief of Naval Operations." *Military Information Technology Q&A, vol. 2 no. 2,* April-May, 1998.

[7] R. Smith, (2000). *Simulating information warfare using the HLA management object model.* SIW Discussions [Spring]. Available: http://www.modelbenders.com/papers/00F-SIW-021.pdf. Retrieved on October 3, 2011.

[8] C. Shannon, *Bell System Technical Journal.* pp. 379-423, July 27, 1948.

[9] C. Kopp, "Information Warfare," Part 1. *A Fundamental Paradigm of Infowar.* Sydney, Australia: Carlo Kopp, & Auscom Publishing, 2000.

[10] S. Al-Fedaghi, "Information Warfare: Definition and Model," New York, USA, submitted, 2009.

[11] C. Kopp, *Journal of Information Warfare,* vol. 2 no. 2, pp. 342-351, 2003.

[12] D. Burke, (1999). *Towards a Game Theory Model of Information Warfare (Thesis).* Air University, Air Force Institute of Technology Web site. Available: https://www.hsdl.org/?view&did=3349

[13] S. Al-Fedaghi, Proceedings from: *the IEEE 32nd Annual Computer Software and Applications Conference.* Turku, Finland: IEEE, 2008.

[14] S. Al-Fedaghi, and F. Al-Azmi, "Evolution of data into an information hierarchy," *Journal of Convergence of Information Technology,* vol. 6 no. 2, pp. 9–21, 2011.

[15] S. Al-Fedaghi, "The Special Interest Group for Design of Communication"

in *Proc. SIGDOC ’08*: Lisbon, Abbrev. Portugal: ACM, 2008.

[16] L. Lamport, “Communications of the ACM,” vol. 21 no. 7, pp. 558-565, 1978.

[17] S. Gosh, “Distributed Systems - an algorithmic approach,” London, UK: Chappman & Hall/CRC Computer and Information Science, 2006.

[18] C. Kopp, and Shannon, “Hypergames and information warfare,” in *Conf. 3rd Australian Information Warfare and Security,* SCSSE. Monash University, Australia, pp. 342-351, 2002.

[19] Y. Moses, et al. “Symposium on Principles of Distributed Computing.” In Proc. *PODC: ACM,* 1985.