Defence Science Journal, Vol. 67, No. 3, May 2017, pp. 282-290, DOI : 10.14429/dsj.67.10051

A Game Theoretic Approach to Modelling Jamming Attacks in Delay Tolerant Networks

Monica Ravishankar[!,*], D. Vijay Rao[#], and C.R.S. Kumar[!]

[!]*Defence Institute of Advanced Technology, Pune - 411 025, India*
[#]*Institute of Systems Studies and Analyses, Delhi - 110 054, India*
[*]*E-mail: monica_pcse14@diat.ac.in*

ABSTRACT

The delay-tolerant-network (DTN) model is becoming a viable communication alternative to the traditional infrastructure model for military, terrestrial and atypical networks, which are characterised by transmission delay and intermittent network connections. The possibility of limited connectivity and resource scarcity in DTNs make them vulnerable to various cyber-attacks, including interference attacks such as jamming. We study the defence against jamming attacks in a delay tolerant network with two adversarial players - the jammer, and the transmitter-receiver pair in a game theoretic environment. The transmitters seek to choose an optimal time to schedule the transmission securely to maximise the probability of successful delivery before the session expires, while signal interferences from the jammer attempts to minimise this probability. We design strategies for the transmitters that offset transmission period based inference of network traffic by the jammer. We deduce a solution for this game, using a probability distribution function over finite number of strategies for both the players to compute their expected payoff. Using a simulation test-bed, we create several scenarios in which the players are considered to have perfect/imperfect information and compute the expected payoff and resulting equilibrium values. The cases of perfect /imperfect information of the players are further studied using entropy based measures. These results are used to strategically evaluate the optimal time for the players, and assess the efficiency of the strategies used by the transmitters against jammer attacks.

Keywords: Delay tolerant networks; Timing constraint; Jamming attacks; Game theory; Optimal strategies

NOMENCLATURE

x	Optimal time for defender to start the transmission
y	Optimal time for the attacker to intrude
d	Network delay set by the network designer
w_t	Waiting time
T	Session time
v	Expected value of the game
$H(x)$	Probability for the defender player to transmit at time x
$P(y)$	Probability of intrusion time y by the attacker player
$I_A(x)$	Step function for choosing a random point x on line interval

1. INTRODUCTION

Military Ad-Hoc networks, Sensor and Sensor/Actuator networks and a typical media networks are a class of challenged networks that arise as a result of time delays, various forms of host-router mobility and frequent network disconnections due to power management and interference[1]. With increasing reliance of military and civilian applications on wireless sensor networks, makes these networks vulnerable to intermittent network connections and transmission delays. However, the widely used internet protocols may not be applicable to networks characterised by long delay and inconsistent connectivity[2,3]. Such networks require protocols that consider connectivity, time delays, reliability and quality of service. Delay tolerant network (DTN) paradigm serves as a means for such networks and regions with mismatched time delays[4,5]. The possibility of resource scarcity in DTNs make them vulnerable to various cyber-attacks, including interference attacks, typically referred to as jamming[6,7]. In the simplest form, jamming is a denial of service attack, considering the role of an adversary, which blocks legitimate communications by flooding the network with jamming waveforms and pulses. In this paper, we focus on the transmitter-receiver pair and jammers that learn the transmission pattern of the network users and frame their jamming strategies so as to intensify the damage in a delay tolerant wireless network. We study the conflict between the defender (transmitter-receiver pair) and the attacker (jammer) in wireless networks that is used to provide delay tolerant internet connectivity. Though security systems are designed against the attacks of the highly skilled adversaries, they are vulnerable to cyber threats. A game theoretic model to study the conflict between the transmitter-receiver pair and jammer in a jamming scenario is proposed. Although ad-hoc

Received : 02 May 2016, Revised : 07 December 2016
Accepted : 20 January 2017, Online published : 24 April 2017

security solutions like cryptography have been traditionally used to protect the confidentiality of the information based on encryption, the knowledge of transmission period can divulge critical and decisive information of the data flow. Owing to this insecure medium of communication, security decisions are investigated analytically using game theoretic models that capture the adversarial nature in jamming scenario. We consider a delay-tolerant sparse network in which a source (set of transmitters) transmits data through the intermediate nodes in the communication range to the destination (receivers). This is done with an aim of achieving successful transmission of the data to the destination (receiver) within a prescribed deadline; however these transmissions are subject to intervention from jammers. We model the two adversary players: the attacker and the defender with conflicting objective as the probability of transmission at each time instant. Transmission at a time t is considered successful when the transmitter attempts transmission in the absence of any intrusion (when the jammer is silent). We design transmission strategies for the transmitter that offset the transmission period based interference of network traffic by jammers. We model and analyse the decision making processes and interactions between the jammer and the transmitter as a game where the strategy of the transmitter is to choose an optimal time to schedule his transmission before his session expires. Conversely, the goal of a jammer is to frame optimal strategies to intensify the damage of the transmission pattern. We deduce a solution for this game, using a probability distribution function over finite number of strategies for both the players to compute their expected payoff. The scenarios in which players are considered to have perfect or imperfect information are studied using entropy based measure

We design a simulation test-bed using Matlab, and create several scenarios in which the players are considered to have perfect/imperfect information using entropy based measures. We then compute the expected payoff and the resulting equilibrium values. These results are used to strategically evaluate the optimal time for the players, and evaluate the efficiency of the strategies used by the transmitters against jammer attacks. The proposed methodology is illustrated using several cases.

2. BACKGROUND STUDIES

Several researchers have studied the application of game theoretic frameworks for solving security related jamming problems in wireless networks with delay tolerance capability. Jamming attacks have been considered in DTNs with its impact on the performance and network operations. Kuriakose and Daniel[8] propose an intrusion detection scheme to monitor the DTN environment for flooding attacks. A table based strategy is proposed by Saha[9] to record the network behaviour and eliminate those nodes detected as malicious. Many analytical tools such as decision theory, machine learning, pattern recognition, and control theory have been used to scrutinise and model the decision making problems in security. Amongst these, game theoretic models seem very effective in assessing and capturing the nature of adversaries, typically classified in the military domain as Red-Teaming strategies. Since game-theoretic methods stand out for their obstinacy, they have a striking virtue to anticipate and design defense against a sophisticated attacker, rather than responding randomly to a specific attack[10,11]. Alain[12] provides a detailed report in which game theoretic models are used to investigate cyber-defence scenarios, while Alpcan and Basar[13] discusses a comprehensive game theoretical structure that models the interaction between the two opposing players. Zhu[14,15] uses game theoretic techniques to analyse the complex decision making processes and interactions between the players. The surveys[16,17] provide a structured and a comprehensive overview of research on the current status of this new field in various research contexts.

Altman and Basar[18] considers the application of game theory to multi-attribute decision problem that arises in a delay tolerant network. Benromarn and Komolkiti[19] propose a game theoretic framework for solving jamming in a delay tolerant wireless mesh network. Azouzi[20] discusses the application of game models to route control in DTN in order to achieve successful and timely delivery of message to the destination with a high probability.

3. PROBLEM DESCRIPTION

Consider a delay tolerant network modelled as a graph of n mobile relay nodes with a low degree of connectivity. The network serves as a gateway that enables communication scenario between the transmitter and receiver nodes, while a Jammer j aims at disrupting their communication intermittently Fig. 1.

The network transmitters (defender) and jammers (attacker) have conflicting interests; where the former aims

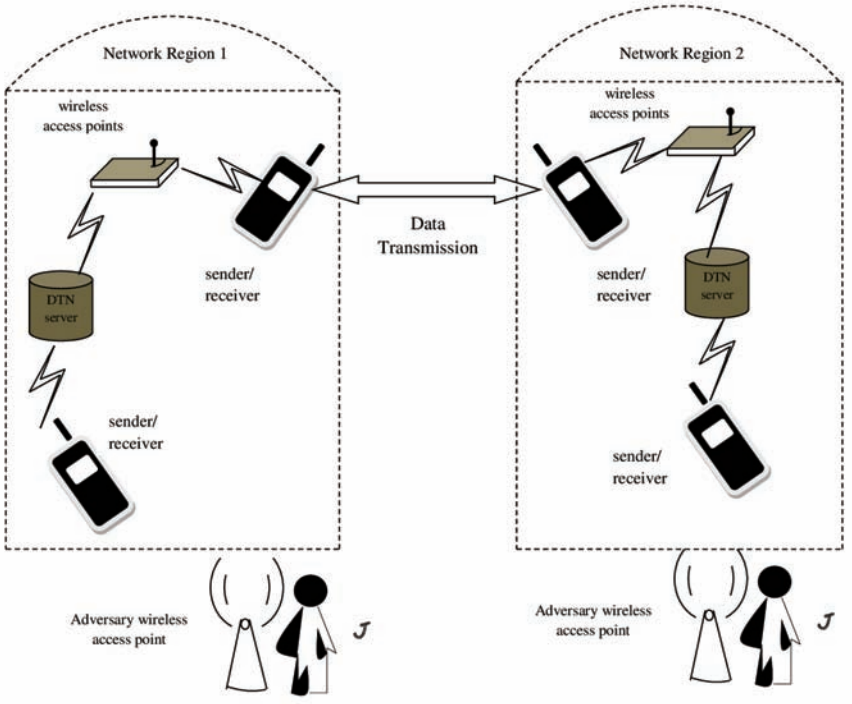


Figure 1. Jamming scenario in a DTN.

to maximise the probability of successful transmission while safeguarding the secrecy while the latter aims to minimise it. Transmission at a time is considered successful only when the network user attempts transmission in the absence of any intrusion.

Strategies: The strategy for the defender is the choice of an appropriate time *X* to schedule his transmission. Since we have considered a delay tolerant network here, we regard the network delay as the waiting time w_t of the packets at each intermediate node (relay), where $0 \le X \le T-d$. Similarly the strategy for the attacker is an appropriate time *Y* for the intrusion, where $0 \le Y \le T$.

Payoff: As stated above, the transmission at a time *X* is successful only when the defender attempts transmission in the absence of jamming. The payoff to the defender player be will be assigned 1 if he transmits the packet before the session time *T* in the absence of any network intrusions and 0 otherwise.

Each player chooses a strategy from a finite set of strategies represented by a point on the closed interval [0,1]. Let

$$w_t = \frac{d}{T},\ x = \frac{X}{T} \text{ and } y = \frac{Y}{T}.$$

This signifies that defender chooses a strategy *x* from a given set of strategies which range over the interval [0,1]. The choices of *x* and *y* (optimal time for defender to start the transmission and optimal time for the attacker to intrude), determines a play of the game, whose outcomes are measured by the payoff function *U(x,y)* which is given by

$$U(x,y) = \begin{cases} 1, & If \begin{pmatrix} [y \le x \le 1-w_t] \\ or \\ [x+w_t \le y \le 1] \end{pmatrix} \\ 0, & If \quad x = y \end{cases} \tag{1}$$

This can be solved by using probability distribution function over finite number of strategies. A mixed strategy for a player *i* is a probability distribution over his pure strategies. This notion of mixed strategies for finite games can be further generalised. Suppose the strategy set for player *i* is finite, then the mixed strategy is a finite distribution over *Y*. This is a distribution that gives a probability value to a finite set of pure strategies. So let $Y_i = \{y_{i1}, y_{i2}, ..., y_{im}\}$ be player *i*'s finite set of points along with the probabilities summing to one. This is done with the understanding that mixed strategy for player *i* is chosen with the probability such that, $q_i = \{q_1(y_{i1}), q_2(y_{i2}), ..., q_n(y_{im})\}$ which is the probability over Y_i, where $q_i(y_i)$ is the probability that player plays Y_i Thus probability distribution over a finite set of points Y_i is expressed as,

$$\sum_{y_i \in Y_i} q_i(y_i) = 1 \tag{2}$$

This signifies the sum of $q_i(y_i)$ over all the $y_i \in Y_i$ so let us denote the set of finite distributions on *Y* by $Y^*(i)$.

Let *H(x)* be the probability distribution functions for the defender player to transmit at time *x* and *P(y)* be the probability of intrusion time *y* by the attacker player. Thus the expected payoff to the defender is as follows:

$$\max_H \min_P E(H,P) = \int_0^{1-w_t} \int_0^1 U(x,y)\,dP(y)\,dH(x) \tag{3}$$

$$\begin{aligned} &= \int_0^{1-w_t} \int_0^x dH(x) + \int_0^{1-w_t} \int_{x+w_t}^1 dP(y)\,dH(x) \\ &= \int_0^{1-w_t} [P(x)+1-P(x+w_t)]\,dH(x) \\ &= \min_y \max_{0\le x\le 1-w_t} [P(x)+1-P(x+w_t)] \end{aligned} \tag{4}$$

This can be written in the following form

$$\begin{aligned} &1 - \max_y \min_{0\le x\le 1-w_t} [P(x+w_t)-P(x)] \\ &= \min_x \int_0^{1-w_t} F(x)\,dH(x) = \min_x F(x) \end{aligned} \tag{5}$$

The given function *F(x)* is continuous in the interval [0, 1-w_t] Thus for the given interval, let the maximum occur at *a*. Then,

$$\min_x F(x) = F(a) \tag{6}$$

Thus,

$$\min_{0\le x\le 1-w_t} \left[P(x+w_t) - P(x)\right] = P(a) \tag{7}$$

Hence,

$$\begin{cases} P(a) \le P(x+w_t) - P(x) \\ \qquad or \\ P(x+w_t) \ge P(x) + P(a) \\ \qquad \forall x\ in\ [0, 1-w_t] \end{cases} \tag{8}$$

Hence, for all the values of *x*, which is iterated from 0 to *(n-1)*w_t (i.e., $i \to 0\ to\ (n-1)w_t$), we obtain $P(nw_t) \ge P(na)$, where $nw_t \le 1 \le (n+1)w_t$. This implies $n = 1/w_t$ and it can attain maximum at $1/w_t$. Therefore we have $P(a) \le 1/n$, which follows

$$\max_y \min_{0\le x\le 1-w_t} \left[P(x+w_t) - P(x)\right] \le 1/n \tag{9}$$

Now, suppose $1/w_t$ is an integer or $nw_t = 1$. Then consider the distribution function $P(y) = y$, where we have,

$$\begin{aligned} E(H,y) &= \max_y \min_x \left[P(x+w_t) - P(x)\right] \\ &= \frac{1}{n} \end{aligned} \tag{10}$$

If $1/w_t$ is a non integer, we use step function to assist us in computing the distribution function which is generally written as

$$F(x) = \sum_{i=0}^{n} a_i Z_{A_i}(x) \tag{11}$$

where $n \ge 0$, $a_i \to$ real nos. and $A_i \to$ Intervals.

Now let us write Z_{A_i} as I_A which is an indicator function of *A* such that,

$$I_A(x) = \begin{cases} 1, & If\ x \in A \\ 0, & Otherwise \end{cases} \tag{12}$$

Thus the distribution function is given by,

$$F(x) = a_i I_{x_i}(x), \ldots\ldots a_n I_{x_n}(x) \tag{13}$$

where $\sum a_i \to 1, \quad 0 \le x_i \le x_{i+1}$

Here we make use of the step function for choosing a point at random on a line interval. Now consider the distribution function

$$P(y) = \sum_{i=1}^{n} \frac{1}{n} I_{\frac{i}{n+1}}(y) = \frac{1}{n} \sum_{i=1}^{n} I_{\frac{i}{n+1}}(y) \tag{14}$$

where $\frac{\mathrm{i}}{\mathrm{n}+1} \to$ intervals.

Hence,

$$P(x+w_t) - P(x) = \frac{1}{n} \sum_{i=1}^{n} \left[I_{\frac{i}{n+1}}(x+w_t) - I_{\frac{i}{n+1}}(x) \right] \tag{15}$$

Since we have,

$$\min_{0 \le x \le 1-w_t} \left[P(x+w_t) - P(x) \right] = \frac{1}{n} = \frac{1}{\left(\frac{1}{w_t} \right)} \tag{16}$$

This game has a value, which is given by

$$v = 1 - \frac{1}{\left(\frac{1}{w_t} \right)} \tag{17}$$

Thus, an optimal strategy for the defender is given by

$$H^*(x) = \frac{1}{n} \sum_{i=0}^{n-1} I_{iw_t}(x) \tag{18}$$

Similarly, an optimal strategy for the attacker is given by

$$\begin{cases} (i) P^*(y) = y & \text{If } nw_t \text{ is an integer} \\ (ii) P^*(y) = \frac{1}{n} \sum_{i=1}^{\frac{1}{w_t}} I_{\frac{i}{\frac{1}{w_t}+1}}(y) & \text{If } nw_t \text{ is non integer} \end{cases} \tag{19}$$

For the defender player we can also further verify that H^* is optimal for which again the following two cases will be considered where (i) $nw_t = 1$ and (ii) nw_t is a non integer. Now suppose $w_t = \frac{1}{n} \text{or} \frac{1}{w_t}$ is an integer, then according to Eqn. (4)

$$\int_0^{1-w_t} \left[P(x) + 1 - P(x+w_t) \right] dH^*(x) \tag{20}$$

$$= 1 - \int_0^{1-w_t} \left[P(x) + 1 - P(x+w_t) \right] dH^*(x) \tag{21}$$

$$= 1 - \frac{1}{n} \sum_{i=0}^{n-1} \int_0^{1-w_t} \left[P(x+w_t) - P(x) \right] dI_{iw_t}(x) \tag{22}$$

$$= 1 - \frac{1}{n} \sum_{i=0}^{n-1} \int_0^{1-w_t} \left[P(iw_t + w_t) - P(iw_t) \right] \tag{23}$$

$$= 1 - \frac{1}{n} \left[P(1) - P(0) \right] = 1 - \frac{1}{n} = 1 - \frac{1}{\frac{1}{w_t}} \tag{24}$$

Now if, $\frac{1}{n+1} \le w_t \le \frac{1}{n}$;

$$E(H^*, P) = \int_0^{1-w_t} \left[P(x) + 1 - P(x+w_t) \right] dH^*(x) \tag{25}$$

$$= 1 - \frac{1}{n} \sum_{i=0}^{n-1} \left[P(iw_t + w_t) - P(iw_t) \right] \tag{26}$$

$$= 1 - \frac{1}{n} \left[P(nw_t) - P(0) \right] \ge 1 - \frac{1}{n} = 1 - \frac{1}{\frac{1}{w_t}} \tag{27}$$

On converting all the values in terms of the original parameters, the solution of the game is:

(i) Value of the game

$$v = 1 - \frac{1}{\left\lceil \frac{T}{d} \right\rceil} \tag{28}$$

(ii) Defender's optimal strategy

$$H^*(X) = \frac{1}{\left\lceil \frac{T}{d} \right\rceil} \sum_{i=0}^{\left\lceil \frac{T}{d} \right\rceil - 1} I_{\frac{id}{T}}(X) \tag{29}$$

(iii) Attacker's optimal strategy

$$\begin{cases} (i) P^*(Y) = Y & \text{If } \left\lceil \frac{T}{d} \right\rceil \text{ is an integer} \\ (ii) P^*(Y) = \frac{1}{\left\lceil \frac{T}{d} \right\rceil} \sum_{i=1}^{\left\lceil \frac{T}{d} \right\rceil} I_{\frac{i}{\left\lceil \frac{T}{d} \right\rceil + 1}}(Y) & \text{If } \left\lceil \frac{T}{d} \right\rceil \text{ is non integer} \end{cases} \tag{30}$$

To summarise, the jamming attack is modelled as follows: Initially, the defender player choses a strategy *X* from the given set of strategies to schedule the transmission. Similarly the strategy for the attacker is an appropriate time *Y* for the intrusion. The choices of *X* and *Y* determine the outcome of the game given as the payoff function Eqn. (1). Next the value of the game is deduced Eqn. (28) and the optimal strategies for the respective players is given by the probability distribution functions *H(x)* and *P(y)* respectively Eqns. (29)-(30). The proposed algorithm is summarised in (Algorithm 1).

Algorithm 1. Transmitter jammer game

1 $d \leftarrow$ network delay
2 $T \leftarrow$ network session time;
3 $X \leftarrow$ defender's choice of time to schedule his transmission;
4 $Y \leftarrow$ attacker's choice of time for intrusion
5 $v \leftarrow$ value of the game;
6 $H(x) \leftarrow$ defender's probability distribution function to transmit at time x;
7 $P(y) \leftarrow$ attacker's probability distribution function to intrude at time y;
8 Initialise the expected payoffs
9 **while** $(y \le x \le 1 - w_t \,||\, x + w_t \le y \le 1)$ **do**
10 **for** $x \in A$ **do**
11 $I_A(x) = 1$;
12 **end for**
13 **for** $x \in [0, 1 - w_t]$ **do**
14 $v \leftarrow$ value of the game
15 $H(x) \leftarrow$ Defender's payoff
16 $P(y) \leftarrow$ Attacker's payoff
17 **end for**
18 **end while**

4. SIMULATION SETUP

We design a simulation test-bed using Matlab, and create several scenarios in which the players are considered to have perfect/imperfect information and compute the expected payoff and resulting equilibrium values. The cases of perfect / imperfect information of the players are further studied using entropy based measures.

4.1 Time Delay – Known or Unknown

In delay tolerant networks, if the employed crypto technique, senses any network intrusions, it eventually delays the network traffic (communication of the normal user) by buffering it for $d = 1, 2, \ldots, T$, which is a design parameter that is set in advance. In practice, any crypto tool requires introducing a short delay in to the system, whose value is set by the network designer.

Case 1: Fixed time delay and known

For illustration purpose, let us assume the delay value set by the network designer is 2 s (assumed to be fixed and known). Then the expected payoff to the defender is 0.034 with the probability 0.2. This is depicted in Fig. 2, where the expected payoff of the defender is shown as the probability function (assumed to be uniformly distributed) for choosing a strategy x from the given set of strategies which range over the interval [0,1] by a random process H. The choices of x, determine the play of the game. Any changes (increase or decrease) in delay has a direct influence on the waiting time (i.e., delay is directly proportional to the waiting time).

Case 2: Uniformly random time delay and Unknown

A more realistic game is one where the delay is randomly chosen by the employed crypto technique. In such a dynamic situation, the delay value is subjected to variation at each time iteration of the network session T as portrayed in Fig. 3.

In practice, the players may start with all the strategies having equally likely probability of usage (a uniform distribution), however, over time, the players will have different probability distributions for the selection of strategies. This signifies different probabilities of attack/defend success or failure for various possible complex combinations of player's actions to obtain effective strategies.

As can be inferred, the strategy for the defender player is the choice of time x to schedule his transmission. Likewise, the strategy for the attacker player is the choice of time y to intrude the transmission. The phenomenon that we observe in Fig 4. portrays $H(x)$ and $P(y)$ (probability distribution functions for the defender and attacker players respectively), used to obtain the optimal time of play for both the players.

Case 3: Time delay is Non-uniformly Random and Unknown

Let us assume the case where the players choose the strategies using non uniform probability distribution. In this scenario, the delay value is subjected to non homogeneous variations at each time iteration of the network session T as portrayed in Fig 5.

4.2 Entropy based Information about the Adversary

Expected payoff is computed by choosing a strategy x from the given set of strategies over the interval [0,1], using uniform probability distribution function. The uniform distribution is the maximum entropy distribution of any interval [a,b].

Then the probability distribution function on $\{x_1, x_2, \ldots, x_n\}$ with maximum entropy[21] turns out to be the one that corresponds to the least certainty of $\{x_1, x_2, \ldots, x_n\}$.The probability distribution functions on $\{x_1, x_2, \ldots, x_n\}$ is the set of positive real numbers $p_1, \ldots, p_n$ that sum up to 1. Entropy is a continuous function of n-tuples $\{p_1, p_2, \ldots, p_n\}$ where the entropy is maximised at $\{\frac{1}{m}, \frac{1}{m}, \ldots, \frac{1}{m}\}$.

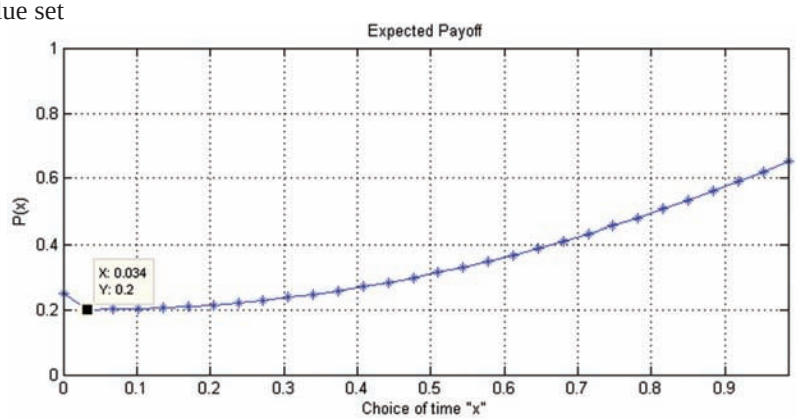


Figure 2. Expected payoff of the defender.

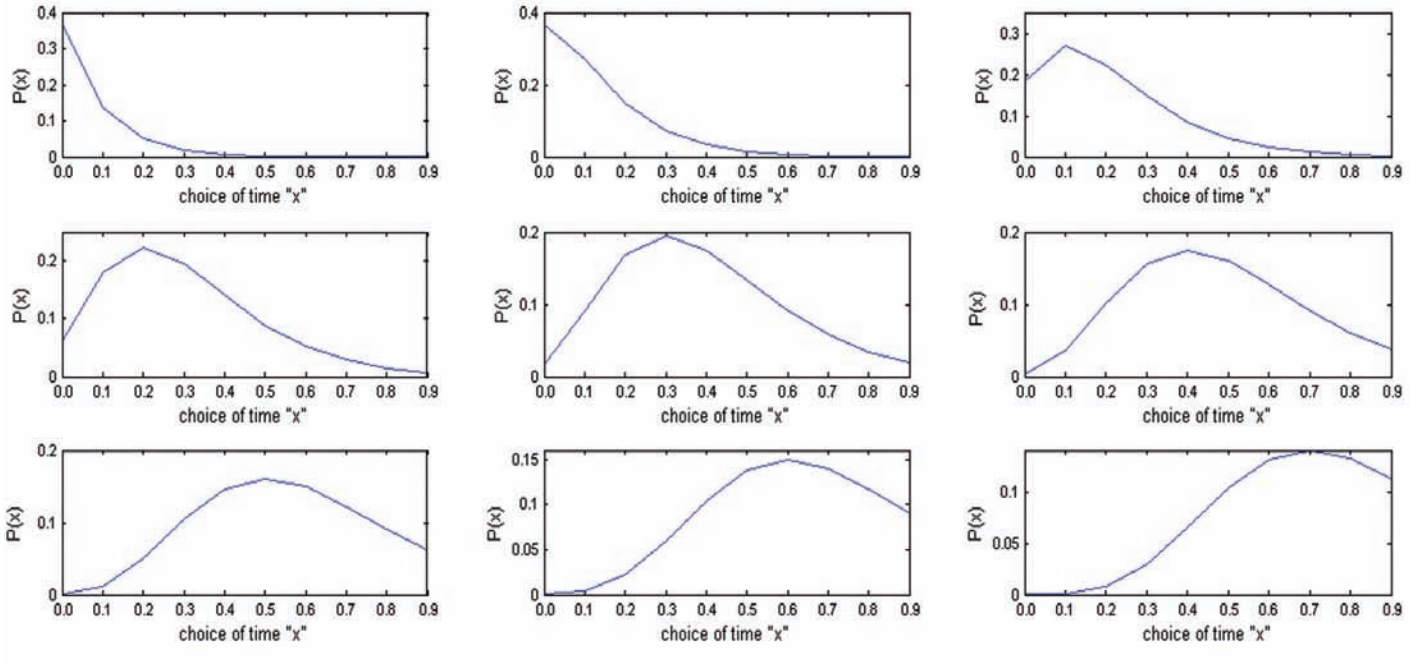


Figure 3. Dynamically varying delay value - uniformly random.

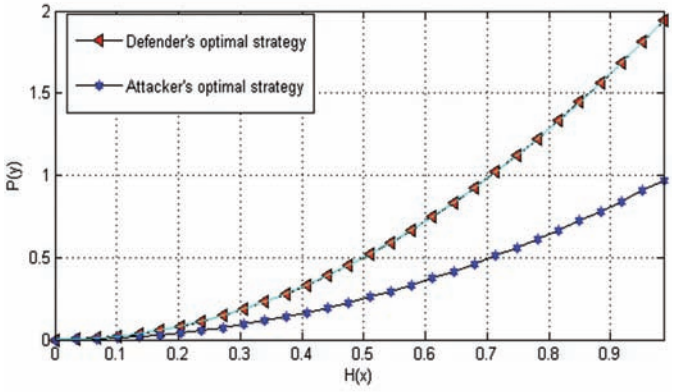


Figure 4. Optimal strategies for the players.

Minimum entropy occurs when the player anticipates about his opponent's moves accurately. In this case, one strategy among the prescribed strategy set is selected with probability 1 and the rest are set to 0's. If the player is uncertain about his opponent's moves then all the strategies x_i are picked with equal probability $\frac{1}{m}$ resulting in maximum entropy. Now let $p(x)$ and $q(x)$ be continuous probability functions over the interval [0,1] and $p(x) = q(x)\ \forall x$. Then let p be any probability distribution function on $\{x_1, x_2, \ldots, x_n\}$ with $pi = p(x)$ letting $q_i = \frac{1}{m}, \quad \forall i \quad -\sum_{i=1}^{m} p_i \log\log q_i = \sum_{i=1}^{m} p_i \log\log m = \log\log m$ which is the entropy of q.

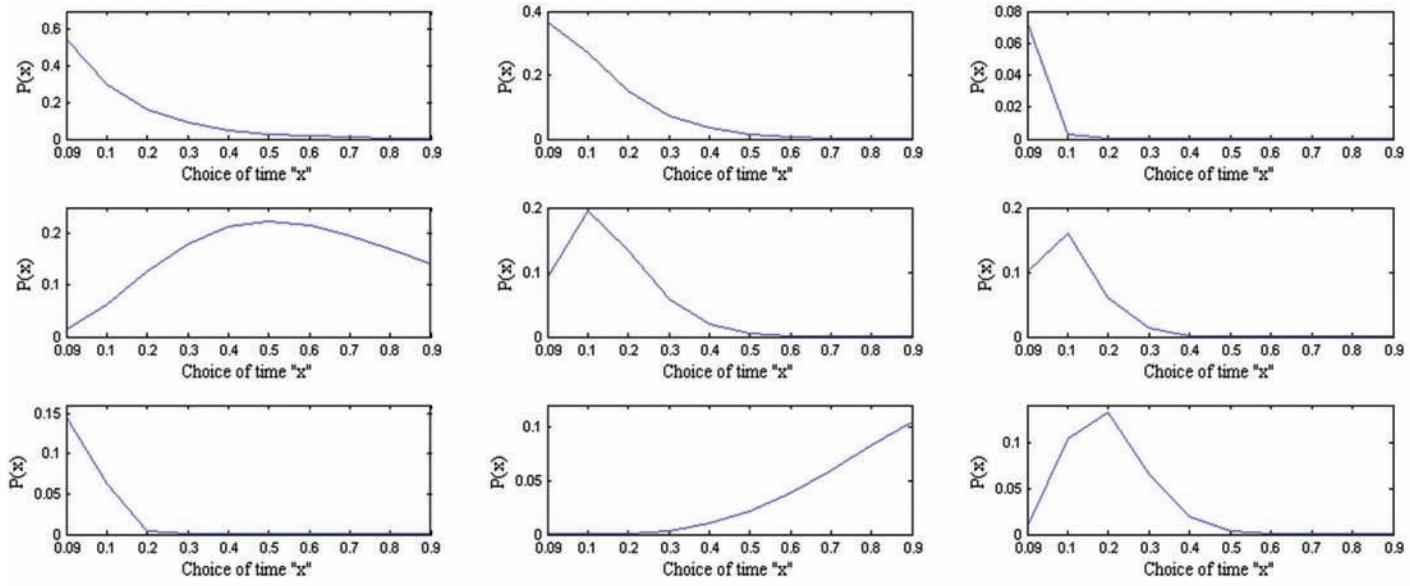
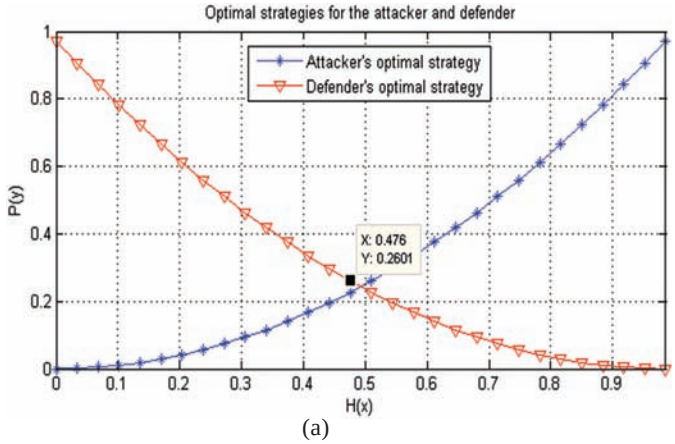


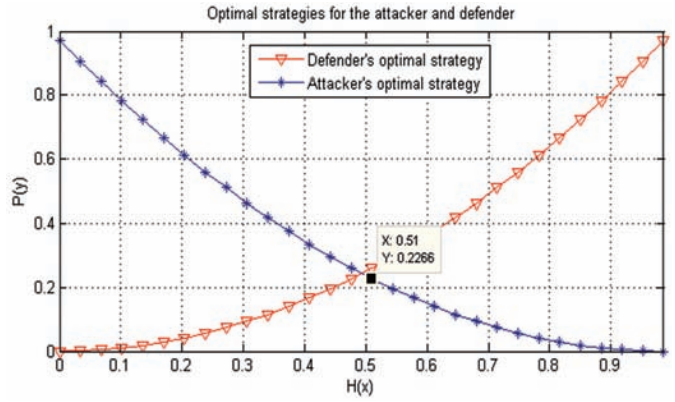
Figure 5. Dynamically varying delay value - non uniformly random.

Case 1: Player has a priori information about opponent

We start with the case where the players are provided with either imperfect information or perfect information of their opponents. If the defender's initial strategy is 0, it signifies that he has zero knowledge of his opponent, while 1 signifies that the defender has perfect knowledge of the attacker. As can be seen from the Figs. 6(a) and 6(b), the attacker starting with the probability 1 and the defender with probability 0, intercept at a point to produce the saddle point of 0.51 for the game. In the next scenario, we try to change the initial condition for both the players and arrive at the same saddle point approximately. Thus the game played is a fair game.



(a)



(b)

Figure 6. (a) Attacker starting with probability 1 and defender with 0 - saddle point 0.51 (b) Attacker starting with probability 0 and defender with 1 - saddle point 0.47.

When the player has imperfect information about his opponent's moves, then the probabilities on his strategy set have equal values of 1/*m* with maximum entropy. If the number of strategies prescribed to the respective is player is 10, then the entropy value computed as log(*m*) is given as 1. Now let us assume that the player has a perfect information about his opponent's moves. Then he is certain about information he will get by choosing each strategy from the strategy set. To illustrate, for the set $X = \{ x_1, x_2, ..., x_{10} \}$, the probability of random selection of each strategy is given by $S = \{\frac{4}{10}, \frac{7}{10}, \frac{8}{10}, \frac{1}{10}, \frac{4}{10}, \frac{4}{10}, \frac{6}{10}, \frac{1}{10}, \frac{1}{10}, \frac{7}{10}\}$ In this illustration there are five different outcomes when each strategy is selected. For which the entropy equals 1.92. This signifies, each time a strategy is chosen from the given set, the amount of information obtained is 1.92 with minimum entropy.

Now letting one player be informed of his opponent's actions, yield optimal solutions, depicted in Fig. 7, which are different from those obtained from the game discussed in previous case.

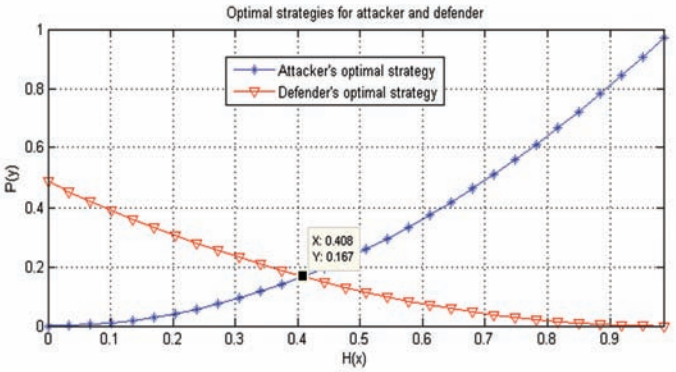


Figure 7. Attacker starting with probability 0.5 and defender with 0 - saddle point 0.41.

Case 2: No a priori information of adversary

In general, if the players lack information, then it is more natural for them to fear the worst from the opponents and reach suboptimal solution. If initial delay is random then suboptimal cases may arise. The initial time delay set by the network user should not be known to the attacker. If by some means, he knows the delay then the probability of intrusions are maximum. If the network is free from attack, the defender can choose any strategy with confidence. If the network is not free from attack, initially due to attacker's actions the defender cannot succeed.

5. CONCLUSIONS

Analysed game-theoretic techniques to model the decision making processes and interactions between the jammer and the transmitters in a delay tolerant network. We obtain a solution for this game, by using probability distribution function over finite number of strategies for both the players to compute their expected payoff. Using simulation techniques, we compute the expected payoff along with the resulting equilibrium. The results are further analysed and discussed for various cases using entropy based measures. These results can be used to strategically decide on the optimal time for both the players.

The game is modelled such that the actions of both the players, i.e., is the probabilities of transmission and jamming *H(x)* and *P(y)* respectively and the network size remain constant over time. In a dynamic model, where the actions of the players that may change in time is dependent on the value of the network state. This is attempted as a future research work, where we consider 'mean fixed game theory' for large number of nodes.

REFERENCES

1. Venkataraman, V.; Acharya, H.B.; Shah, H.; Lam, S. Delay tolerant networking – a tutorial. 2009.
2. Sun, W.; Liu, C. & Wang, D. On delay-tolerant networking and its application. *In* Proceeding of 2011 International Conference on Computer Science and Information Technology (ICCSIT 2011). doi: 10.7763/IPCSIT.2012.V51.42.
3. Raveneau, P.; Chaput, E.; Dhaou, R. & Beylot, A. DTN for WSN: FREAK, implementations and study. *In* Proceedings of 12th IEEE workshops on Consumer Communications and Networking Conference, 2015. doi: 10.1109/CCNC.2015.7157939.
4. Ntareme, H.; Zennaro, M. & Pehrson, B. Delay tolerant network on smartphones: Applications for communication challenged areas. *In* Proceedings of the 3rd ACM Extreme Conference on Communication: The Amazon Expedition. doi: 10.1145/2414393.2414407
5. Xiao, M.; Wu, J. & Huang, L. Community-aware opportunistic routing in mobile social networks. *IEEE Trans. Comput.*, 2014, **63**(7), 1682-1695. doi: 10.1109/TC.2013.55
6. Peng, W.; Li, F,; Zou, X. & Wu, J. Behavioral malware detection in delay tolerant networks. *IEEE Trans. Parallel Distributed Sys.*, 2014, **25**, 135-148. doi: 10.1109/TPDS.2013.27.
7. Niyato, D.; Wang, P.; Kim, D.I.; Han, Z. & Xiao, L. Performance analysis of delay-constrained wireless energy harvesting communication networks under jamming attacks. *In* Proceedings of 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, 2015, pp. 1823-1828. doi: 10.1109/WCNC.2015.7127745
8. Kuriakose, D. & Daniel, D. Effective defending against flood attack using stream-check method in tolerant network. *In* Proceedings of Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, pp 1-4. doi: 10.1109/ICGCCEE.2014.6921381
9. Saha, S.; Verma, R.; Sengupta, S. & Nandi, S. A strategy for secured routing in spray and focus routing protocol for DTN. *In* Advances in Computing and Information Technology, Springer Berlin Heidelberg, 2012, pp. 159-169. doi: 10.1007/978-3-642-31513-8_17
10. Lye, K-W. & Wing, J.M. Game strategies in network security. *Int. J. Info. Sec.*, 2005, **4**, 71-86. doi:10.1007/s10207-004-0060-x
11. Liu, D; Wang, X. & Camp, L.J. Game theoretic modeling and analysis of insider threats. *Int. J. Critical Infra. Prot.*, 2008, **1**(12), 75-80. doi:10.1016/j.ijcip.2008.08.001
12. Alain, B.; Kantarcioglu M. & Hoe S. A game-theoretical approach for finding optimal strategies in a botnet defense model. *In* Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2010, **6442**, pp. 135-148. doi: 10.1007/978-3-642-17197-0_9
13. Alpcan, T. & Baser, T. Network security: A decision and game-theoretic approach. Cambridge University Press, November 2010.
14. Manshaei, M.H; Zhu, Q.; Alpcan, T.; Basar, T. & Hubaux, J.P. Game theory meets network security and privacy. ACM Computing Surveys, December 2011. doi: 10.1145/2480741.2480742
15. Zhu, Q; Saadz, W; Han, Z; Poor, H.V. & Basar, T. Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach. *In* Military Communications Conference, 2011 - Milcom, 2011, pp. 119-124. doi: 10.1109/MILCOM.2011.6127463
16. Roy, S.; Ellis, C.; Shiva, S.; Dasgupta, D.; Shandilya, V. & Wu, Q. A survey of game theory as applied to network security. *In* Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010. pp. 1-10. doi: 10.1109/HICSS.2010.35
17. Nguyen, K.C.; Alpcan, T. & Basar, T. Security games with incomplete information. *In* IEEE ICC 2009 Proceedings. pp. 1-6. doi: 10.1109/ICC.2009.5199443.
18. Altman, E.; Basar, T. & Kavitha, V. Adversarial control in delay tolerant network. *In* the First International Conference on Decision and game theory for security, GameSec 2010, Berlin, Germany, November 22-23, 2010.
19. Benromarn, S.; Komolkiti, P. & Aswakul, C. Game theoretic analysis of jamming attack in wireless mesh network with delay tolerance. *In* Proceedings of 2013 International Computer Science and Engineering Conference (ICSEC), Nakorn Pathom, 2013, pp. 354-358. doi: 10.1109/ICSEC.2013.6694808
20. El-Azouzi, R.; De Pellegrini, F. & Kamble, V. Evolutionary forwarding games in delay tolerant networks. *In* 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Avignon, France, 2010, pp. 76-84. doi: 10.1016/j.comnet.2012.11.014
21. Ren, F.; Zhao, B.; Yu, H.; Xu, A.; Hao, Y. Theoretical research on structural equation model based on principle of entropy. *In* Proceedings of 2011 International Conference on E-Business and E-Government (ICEE), Shanghai, China, 2011, pp. 1-4. doi: 10.1109/ICEBEG.2011.5881440

ACKNOWLEDGMENTS

The authors would like to gratefully acknowledge Dr Srinivasan Vathsal and anonymous reviewers for fruitful discussions, suggestions and reviews.

CONTRIBUTORS

Ms Monica Ravishankar is pursuing her PhD from Defence Institute of Advanced Technology, Pune. Her research interests include: Operations research and game theory.
Contribution in the current study; she designed of mathematical model, simulation and analysis of data and preparation of the manuscript.

Dr D. Vijay Rao obtained his MS (Engg) and PhD from IISc Bangalore. Currently working as a Scientist with the Institute for Systems Studies and Analyses at Delhi. His areas of specialisation include: Military Systems analysis, design and development of wargames and strategic systems, modelling and simulation of warfare systems and military operations analysis.
Contribution in the current study; he initiated the work, contributed in the design and analysis of data and preparation of the manuscript.

Dr C.R.S. Kumar obtained his MTech from IIT Madras and PhD from University of Melbourne. Currently working as faculty member of Defence Institute of Advanced Technology, Pune. His areas of specialisation include: Jamming/anti-jamming, game theory and cognitive radios networks.
Contribution in the current study; he provided logistic support required for the research