Sādhanā (2019)44:245
https://doi.org/10.1007/s12046-019-1228-4

Using game theory to model DoS attack and defence

BHUPENDER KUMAR* and BUBU BHUYAN

Department of Information Technology, North Eastern Hill University, Umshing Mawkynroh, Shillong 793002, India
e-mail: bhupinder.nayak@gmail.com; b.bhuyan@gmail.com

MS received 3 March 2018; revised 26 August 2019; accepted 4 October 2019

Abstract. Denial of service (DoS) or distributed denial of service (DDoS) attacks based on bandwidth depletion remain a persistent network security threat and have always been an important issue for system administrators and researchers. Defence mechanisms proposed so far to defend against such attacks could not address the problem adequately and efficiently due to lack of quantitative approaches in modelling defence strategies against DoS/DDoS attacks. Game theory is a microeconomic and mathematical tool that provides a quantitative framework to model such attacks. A model based on game theory can act as a decision support system to the defender and augments its capabilities to take best decisions for maintaining an optimum level of network security round the clock against such attacks. Inspired by this, different DoS/DDoS scenarios, where game theory has been used to represent the strategic interaction between the attacker and a defender, are investigated. Based on the strategic interactions, a game theoretical defence mechanism is proposed to mitigate DoS/DDoS attacks. The proposed mechanism is based on two-player zero-sum game. It considers DoS/DDoS attack based on bandwidth depletion where an attacker wants to occupy maximum bandwidth of a link having a limited capacity. The attacker does so by flooding the network with unsolicited or malicious flows. The attacker has to decide an effective attack rate per flow. It has to choose an optimal size of botnet also for a cost-effective attack. It does trade-off analysis prior to attack. If its payoff or benefit obtained is less than the attack cost, it chooses to refrain from launching such a costlier DoS/DDoS attack. On the other hand, to set an upper bound on network traffic, the defender needs to set an optimum threshold per flow so that maximum attack flows are either dropped or redirected to a honeypot deployed in the network. Arbitrary setting of a threshold for flow rates can also cause a loss of legitimate flows. The defender chooses the optimum threshold value with precise estimation to minimize loss of legitimate flows. The defender also does trade-off analysis and sets the threshold in a way that can minimize the attacker's payoff. This optimization problem is presented as a game between the attacker and defender. Action sets and objective functions of both players are defined. The network constrains are modelled and payoffs are calculated. The game converges to Nash equilibrium. The best course of actions is deduced from the Nash strategies. Results obtained by simulation and numerical calculations are in favour of the proposed game theoretical defence mechanism and strongly advocate the worthiness of using game theory to defend against DoS and DDoS attacks to strengthen network security.

Keywords. Denial of service attack and defence; bandwidth; game theory; payoff; Nash equilibrium; optimization.

1. Introduction

With India heading towards complete digitalization and dependency on internet, network has become an indistinguishable part of our day to day life. With increasing dependency on networks, security concerns have also increased manifold. Security of the network is a challenging task because the attackers use new and evolved mechanisms to damage network infrastructures and render services unavailable. These attacks are launched by exploiting some network vulnerabilities or configuration flaws of networked devices. An attack severely affects the confidentiality, integrity and availability (CIA) of data or services, which results in loss of money, data privacy, reputation of an organization, huge damage to infrastructures and unavailability of services for a considerable duration. Denial of service (DoS) attack deprives legitimate and intended users from obtaining the services of a network. If the attack is launched using one machine, it is a DoS attack. If many compromised machines (botnets or zombies) are used to launch the attack, it is called as distributed denial of service (DDoS) attack. One among the first DDoS attacks was

*For correspondence
Published online: 30 November 2019

launched against Yahoo in February 2000, resulting in monetary losses by Yahoo and halting its servers for a significant period of time [1]. DDoS can be launched using social network sites, internet relay chats and other readily available software tools like Trinity V3, Kaiten, BlackEnergy, Low Orbit Ion Cannon (LOIC),[1] Trinoo, Tribe Flood Network (TFN),[2] TFN2K, etc. These tools cause UDP, ICMP, TCP-SYN, TCP-ACK and TCP-Null flood attacks. The DDoS attack can be classified into two broad categories: (1) vulnerability-based DDoS attack and (2) flooding-based DDoS attack. In vulnerability-based DDoS attack, the attacker tries to exploit the vulnerability found in any software, application or protocol of the network under consideration [2]. The flooding-based DDoS attack can be launched by sending large number of packets or SYN requests to a server or the victim machine. Congestion is caused if the total network traffic is more than the capacity of a bottleneck link. It disrupts the connectivity by depleting whole network bandwidth or exhausting resources like router's processing capacity or buffer space, CPU's time or memory, etc. [1, 2]. Some common types of flooding-based DoS and DDoS attacks are given in table 1 as discussed in [1]. Table 2 describes various defence mechanisms proposed in literature against DoS and DDoS class of attacks.

In spite of so many defence mechanisms and better technology, DoS attacks are increasing in size and numbers. Increased size and numbers of DoS have made the detection and defending more difficult. The problem is still an open issue and severe security threat worldwide also because of high speed, complex, distributive and interdependent network structures. Flow-based mechanisms can detect the increased amount of flow rate of packets in the link but do not suggest how to choose a threshold per flow dynamically to prevent DoS attacks. Other network security solutions like firewall and Intrusion Detection Systems or Intrusion Prevention Systems also lack quantitative decision framework for flow rate configuration. Limitations of a few of defence approaches suggested so far are given in table 3.

Avoiding such attacks is very difficult because of the attacker's changing attack behaviour, technological advancements, organized manner to attack and his remote physical locations. Attackers are no more novice and irrationals who attack for fun, reputation or building a superiority among their colleagues. They do cost–benefit or trade-off analysis to gain maximum attack benefits with minimum attack efforts, minimum attack costs and minimum chance of detection by any network security device. The defences approaches as mentioned in table 2 do not consider the attacker's incentives and its trade-off analysis for launching the attack. To defend against DoS/DDoS attacks in such an environment needs defence mechanisms based on quantitative framework that can mathematically model the attacker's objective and its incentives.

[1]Available at https://sourceforge.net/projects/loic0/.

[2]Available at https://packetstormsecurity.com/distributed/tfn2k.tgz.

Game theory has attracted the researcher fraternity and network security engineers because of the mathematical and micro-economical aspects involved in real attack scenario. A network attack always and in almost all cases involves interactions between two or more network agents (players) that have opposite and competitive interests. These network agents can be an attacker and a defender. The probability of successful attack is based on the strategic interactions between the players. Hence, whenever there is a strategic interaction between two or more players, a game is formulated. Both players decide their best response in an attack scenario to maximize their benefits. Using game theoretical model, a defence mechanism can be designed that defines the action space of attacker and defender, their corresponding payoff or utility functions and the best response as Nash equilibrium strategies. Mechanisms based on game theory can suggest how to choose an optimal action dynamically and iteratively. Game theory quantifies the players incentives, gain and losses. The quantification leads to a cost–benefit analysis. If the attack can be made costlier or if the attacker's interests and incentives behind the attack can be decreased, a rational attacker refrains from launching a DoS or DDoS attack. A good work on modelling Attacker's Intent, Objective and Strategies (AIOS) using game theory is carried out in [3]. A detailed survey of using game theory for network security has been carried out in [4]. This work addresses some of the issues raised earlier in traditional defence approaches. Simultaneously, it also incorporates the issues raised in game theoretic defence mechanism proposed in [5]. The main contributions of this work are as follows:

- It proposes a defence mechanism that works as a decision support system to network defender and helps in setting an optimum upper bound or optimum threshold on incoming traffic per flow dynamically. It models the situation as a two-player zero-sum game and optimization is done based on saddle points or Nash equilibrium of the game using simulation and numerical computations.
- The proposed mechanism quantifies not only the network parameters but also the attacker's incentive, its intentions and objectives to understand the real attack scenario in an accurate and efficient way. It models the attack traffic using poisson distribution, computes the probabilities of attack flows to be lesser than or equal to optimal threshold set by defender and defines corresponding payoff or objective functions of the attacker and defender both.

The rest of the paper is organized as follows. Section 2 gives a brief overview of basic principles used in game theory, section 3 presents a detailed study of related work, section 4 describes the proposed network model and section 5 formulates the game between players. Section 6 discusses the experimental results obtained using

Table 1. Some DoS and DoS attacks.

Network or transport Level flooding attack	Spoofed or non-spoofed UDP flood
	ICMP flood, DNS flood
	TCP SYN and TCP-SYN ACK flood
	ACK and Push ACK flood
	RST/FIN attack
	Smurf attack, fraggle attack
Application level flooding attack	HTTP session flooding attack
	HTTP get/post-flooding attack
	HTTP fragmentation attack
	Slowloris attack, slow-reading and slow-response attack

Table 2. Some proposed defence mechanisms.

Network or transport level defence	Ingress or egress filtering
	D-WARD, MLTOPS, TOPS
	MANAnet's reverse firewall
	Packet marking and link testing
	(IP trace-backing)
	History-based IP filtering
	Hop count filtering
	Aggregate-based congestion control (ACC)
	Push-back, attack diagnosis
	Parallel attack diagnosis, TRACK
	COSSACK
	Capability-based mechanism
	Traffic validation architecture
	Stateless internet flow filter,
	Active internet traffic filtering, StopIt
Application-based DDoS defence	DNS amplification attack detector (DAAD)
	DDoS shield, SpeakUp
	Hybrid detection based on trust and information theory

Table 3. Limitation of defence mechanisms.

Ingress or egress filtering	Not effective with genuine IP address spoofing by botnets
D-WARD	More memory consumption and no incentive design
MLTOPS and TOPS	Incoming/outgoing traffic may not be proportional, high false negative rate
MANAnet's reverse firewall	Not dynamically adaptive, no incentive for source that deploys it
Packet marking, link testing	Required large numbers of routers and computational burden
History-based IP filtering	False negative and false positive
Hop count filtering	Hop count mapping may be inaccurate
Aggregate-based congestion control (ACC)	Large distributed attack sources' traffic not identified
Capability-based mechanism	Processing and memory issues

MATLAB and section 7 concludes the paper by giving some ideas for future work in section 8.

2. Fundamental concepts of game theory

2.1 *Definition of a game*

When two or more players interact, a game is formulated. It comprises the following.

- *A set of two or more rational players*: From DoS/DDoS attacks point of view, these players are the attacker versus defender, or botnet versus defender. In case of wireless network, the sensor nodes can be categorized as normal versus malicious nodes. If some defence measures are already in place like IDS or IPS then the set of players can be considered as IDS/IPS versus attacker.
- *A set of actions available to each player*: From DoS/DDoS attacks point of view, the action set can

comprise setting a flow threshold, dropping a flow, letting a flow to pass, redirecting it, setting an optimal botnet size, optimal attack rates, whether to attack or not to attack and forwarding packets or not to forward.

- *A utility or payoff for each subset of action*: The utility is defined as the total benefits minus the total cost obtained by adopting a subset of action. It can be a positive, zero or negative value. From DoS/DDoS attacks point of view, the benefits of the attacker are based on the absolute impact caused on network bandwidth and relative impact on the legitimate flows. However, it can be designed based on suitable situation-specific network parameters like average throughput, transmission delay, SINR ratio, etc. in other cases. Similarly, costs can be quantified and defined in terms of efforts and time utilized for acquiring a bot in case of DoS/DDoS attacks. An objective function is constructed based on the costs and benefits. The objective function can either be maximized or minimized.
- *Nash equilibrium concept of a game*: It is the saddle point strategy of a player that fetches him a maximum possible payoff. If a player chooses to deviate from the Nash strategy, it either gets equal or less payoff. A player cannot get any better payoff by deviating. Nash equilibrium is the solution concept of a game. It suggests the best response to be taken by a defender in case of an attack. For more about game theory, one can refer [6].

2.2 *Different types of games*

- *Cooperative and non-cooperative game*: In cooperative games, communication between the players is allowed. Due to communication, players cooperate with each other and take actions to achieve an optimum goal that is globally accepted and beneficial to all. No communication is allowed between players in a non-cooperative game setting.
- *Zero- and non-zero-sum game*: In zero-sum game, payoffs or utilities of all players are added and it equals zero. This means that the gain of one player is actually a loss to other and vice versa. However, in non-zero-sum game, the payoff of a payer is based on separate network parameters specific only to that player.
- *Static and dynamic game*: Static games are one-shot games where the players take decisions once and for all. In dynamic games, decisions are made sequentially over many stages before the game converges to Nash equilibrium. A player can improve its payoff in subsequent stages of the game.
- *Perfect and imperfect information game*: In perfect information game, a player is always aware of the past actions of other players. However, in imperfect information game, at least one player does not have knowledge of the past action of other players.
- Bayesian game: Bayesian games are incomplete information games where at least one player does not know the payoff function of the other players. A player maintains a belief about the type of other players. The solutions of such games are derived by Bayesian analysis.

3. Literature survey

3.1 *Non-cooperative game modelling*

Yaar *et al* [7] suggested a Stateless Internet Flow Filter (SIFF)-based approach to mitigate the DoS attack. The flows are divided into two categories – privileged flow and unprivileged flow. Authors suggested how the privileged flow can be protected while dropping the unprivileged flow. Xu and Lee [8] suggested a mechanism based on game theoretic approach to defend a web-service under DoS attack. Authors used various matrices of the total throughput of the attacker and legitimate users, number of attackers and legitimate users, packet drop probabilities of both players and the average time taken for downloading a web page by the user. A defence mechanism based on game theory against DDoS attack has been proposed by Bedi *et al* [5]. The work is based on identifying and blocking the traffic of an attacker that causes bandwidth depletion by flooding the network. Probabilistic functions of rate of arrival of legitimate flow are modelled using normal distribution. Based on the statistical interpretation, ratio of lost legitimate flow to total legitimate flow is computed. The thresholds are kept fixed and probabilities of getting a flow passed, dropped and redirected to honeypot are decided based on sigmoid functions. However, dynamic adjustment of threshold for a flow to pass or drop is not discussed, the game is static and attack traffic is not modelled using some probability function like the normal traffic.

A two-player static game has been modelled as the interaction of attacker and defender in [9] comprising the action set of attacker as *Attack, Not attack* and defender as *Defend, Not Defend*. The payoff function is constructed based on the cost of attack, cost of defending and damage inflicted to the system. Mixed strategy Nash equilibrium is calculated to suggest the best action to be taken by the players based on the probability of attack and defend. However, no specific attack was considered in the paper. In 2008, Alpcan and Sonja [10] modelled a game as two-player zero-sum game with complete information for the security of Vehicular Networks (VNET). Attacker wants to jam *a class of DoS attacks* or sybil attacks or tries to disseminate false information in order to disrupt the traffic. Defender mobile nodes want to deploy countermeasures. Authors represented road network, vehicular traffic and

data traffic using graphs. From the graphs, centrality measures showing the importance of road segment are calculated. The centrality measure is used to calculate the payoff of the players, i.e., risk or penalty for attackers if found and benefit for defenders. Attackers jam a road segment with some probability. Defenders allocate defence resources to the same or another segment of road. The outcome of the game is represented using a game matrix containing payoff for actions of players. Game matrix entries are functions of importance of each road segment. Attackers are assumed as row players who want to maximize and defenders as column players who want to minimize harms on the network. Authors proved the existence of Nash equilibrium for the complete information zero-sum game. However, in real scenario, complete information availability to a player before taking an action might not be feasible.

In 2010, Zhu *et al* [11] modelled the jamming and anti-jamming scenario for primary user emulation attack and introduced a stochastic zero-sum Markovian game for cognitive radio systems. Interactions between secondary user and jammer are modelled where the primary user controls the system states and their transitions. The secondary user and jammer are non-cooperative and act against each other in all channel states. Saddle point strategy for secondary user is to improve its spectrum sensing capabilities or choose the communication states where the available channels are less prone to jamming. Payoff of secondary user increases with more availability of jamming-free channels but it can be limited by the behaviour of primary user. This model did not consider the sensing errors or uncertainty. It considers only a single attacker scenario and did not compute the Nash equilibrium of the game.

Game theoretical concept for deception in network is suggested to improve the network security against a variety of attacks. In 2013, Kiekintveld *et al* [12] discussed three game theoretical models, which help the network administrator to decide how to deploy optimal number of honeypots in a network to increases its security. Honeypots are a limited number of fake hosts with minimum information or database, which are introduced in the network to distract the attacker. In 2015, Durkota *et al* [13] developed a network security hardening model as a stackelberg game. Authors showed that the best strategy of defender is placing optimal number of honeypots with vulnerability database in the network so that the honeypots can detect network attack with a maximum probability.

The problem of reliable communication in the presence of active and passive attackers in the network is modelled as stochastic game in [14]. The actions of the attackers are defined as whether to *eavesdrop* the channel or *jam* it. In the first case, attackers face less chances of detection but in the latter scenario, greater risk of detection is involved. For attackers, *eavesdropping* may not be as efficient as *jamming*. The action of the regular user is either to *transmit* or remain *silent* to delay its transmission. The action *transmission* provokes the attacker to adopt *jamming* strategy. The next action of the regular user to strategically allocate *silent* mode while the attacker is still *jamming* would increase the probability of detection of the attacker by IDS. It is showed that under certain conditions, randomizing the strategic use of silent mode increases the optimum level of network security.

3.2 *Cooperative game modelling*

Game theoretical models based on incentives for inducing the users cooperation for increasing the security of wireless channel have been studied in [15–17]. Rational users cooperate to increase the SINR to an optimum level to increase the secrecy capacity of the communication channel between a sources and destination pair while degrading it between sources and eavesdropper. Authors have designed such games between a friendly jammer and regular nodes for cooperative jamming in [15, 16] and between nodes themselves for cooperative spectrum access in [17].

Secure routing protocol based on the collaboration of mobile nodes in Mobile AdHoc Networks is proposed in [18]. The protocol uses dynamic Bayesian signalling game to analyse the strategic profile of regular and malicious nodes and suggests the best actions to be chosen by nodes. Perfect Bayesian equilibrium is computed. It is suggested that the regular nodes should be cooperative during routing and update their payoff and beliefs about the neighbours while malicious nodes try to deviate from the cooperation. Deviation of malicious nodes from cooperation is based on the risk analysis and probability evaluation of detection. Detection of malicious nodes lowers the utility of such nodes. Based on the utility obtained, malicious users are forced to cooperate in secure routing protocol for MANET. In 2015, Abegunde *et al* [19] proposed a deadlock-free Resilient Tit for Tat (RTFT) algorithm as a solution to the wireless MAC layer misbehaviour. Authors used wireless network parameters such as contention window, throughput of channel, power consumption by nodes, etc., to construct the utility function. Simulation showed that it is possible to implement a strategy that makes misbehaviour unattractive, ineffective and less rewarding. Authors proved that by using RTFT, desired level of cooperation can be achieved between nodes of a wireless network to strengthen its security [19].

4. Network model

4.1 *Network topology under consideration*

The network topology considered in this work for analysing DoS/DDoS attack is given in figure 1. The total number of attack nodes is m and each node sends an attack flow at a rate r_i^a where r_i^a denotes the sending rate in bits per second

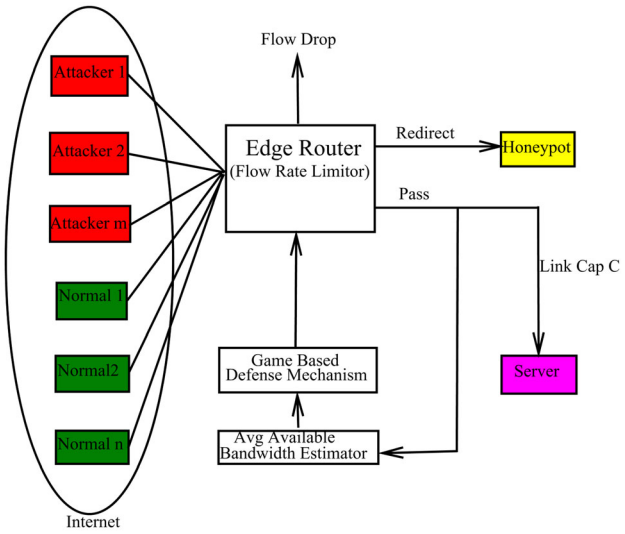

Figure 1. Network topology under consideration.

adopted by i^{th} attack flow and $i = 1, 2, \ldots, m$. Similarly, there are n number of legitimate nodes and each sends a normal flow at a rate of r_j^l where r_j^l denotes the rate in bits per second of j^{th} legitimate flow and $j = 1, 2, \ldots, n$. It is construed that $\forall i, j \mapsto \Re^+$. The number of attack nodes and legitimate nodes may vary according to attack situation. Total numbers of nodes are N, where $N = m + n$. Each node can establish more than one flow between an origin and destination pair but for simplicity of analysis, all flows from a source are aggregated and treated as a single flow having aggregate traffic rate in bps. Total incoming flow f at an edge router is $\sum_{i,j=1}^{i=m,j=n} mr_i + nr_j$ bps. In the topology under consideration, a direct link l between edge router and target server having a capacity C in bits per second is considered. Many links can exist for a flow to travel between a source and destination pair. In case of existence of many links, the bottleneck link can be considered as vital and vulnerable to DDoS attack. The link's bandwidth is shared by all flows equally as in the case of TCP flows. The link l cannot sustain the incoming traffic if $f > C$, resulting in severe congestion at the link and DoS to legitimate users. An Available Bandwidth Estimator (ABE) is placed on the link l, which estimates the average utilization of bandwidth over a time interval. The ABE can be a standalone machine acting as a network manager, and obtains performance information from the database of the link router/client using SNMP queries. The average utilization of the link is used to calculate the average available bandwidth B_{avl} over an interval of interest. The average available bandwidth is calculated in percentage. B_{avl} is passed to game-based defence mechanism. The defence mechanism computes the flow threshold τ dynamically. This dynamic value of τ is based on capacity of link, average available bandwidth, number of total flows and the utility obtained by the defender. The mechanism passes the value of τ to the edge router. The edge router decides whether to allow, redirect or drop a flow based on the value of τ.

4.2 *Assumptions and constraints*

Without loss of generality, some assumptions are made in the proposed model for simplicity of analysis. The proposed defence mechanism is not protocol specific. It can be used for both TCP and UDP flows or till the time a flow behaves in a TCP-friendly manner. The mechanism can also be mapped to other network topology with the central idea unchanged. The few assumptions that would make the analysis simple are as follows:

- Defenders always have a rich set of information about the networked devices, link capacity and current security level of the network under its administration. However, the attacker has to infer the probabilities of its flow to pass, drop or get redirected to honeypot using either history-based heuristic knowledge or some intelligent tools. The attacker needs the information to formulate its payoff function. Accuracy of payoff estimation is directly proportional to accuracy of information inferred from the network.
- The link transmits in half duplex or full duplex mode according to the configuration of transmitter and receiver nodes. In half duplex mode, time division duplexing can be used for upstream and downstream. In full duplex mode, the link uses capacity C for upstream and downstream at the same time. This implies that the whole bandwidth of the link is available for upstream and downstream transmission simultaneously. Choosing a mode of transmission causes no significant effects in the proposed defence mechanism.
- The capacity C of a link does not change very frequently between an origin and destination pair until and unless some new configurations are made in the network or some additional links with more bandwidth are added to it. If such a change takes place in the link's capacity, it directly affects the fair share of bandwidth allotted to a flow and threshold set by the defender as mentioned in Eq. (7) and corresponding payoff of the players.
- An attacker adopts exactly the same function to generate the rate of attack bits per flows from every bot under its control in DDoS attack. The generation function can be normally distributed, poisson process, constant bit rate or increasing with time. The proposed mechanism uses poisson distribution to model attack traffic. The same can be modelled using any other function and it is expected to give similar results. Using different generating functions on each bot is not cost effective for attackers. If somehow, attackers use

such a strategy, modelling of the attack traffic needs to be changed according to the function chosen by the attacker.
- For simplicity, single flow per node is considered. An attack node is able to generate many flows per node but the whole traffic volume generated by all flows is aggregated and considered as a single flow between an origin and destination pair.
- The attacker does not spoof an IP address. If it does so, there exists some security measures to resolve the IP spoofing. If the IP spoofing is not resolved, the mechanism treats the transmission between the spoofed source and destination IP addresses as an independent flow and allots the fair share of bandwidth to it.

4.3 *Average available bandwidth computation*

If the defender has administrative rights, it can easily compute the average utilization and average available bandwidth of a link over an interval of interest using SNMP queries from edge router's information database. If the defender does not have administrative rights to link under consideration, it can still use some publicly available bandwidth measurement tools to measure end to end average available bandwidth. Some of the publicly available tools are *pathchar, pchar, nettimer, pathrate* and *pathload* as discussed in [20]. At a particular instance of time, the link either transmits at its full or remains idle, resulting in an instantaneous utilization equal to 1 or 0, respectively. Instantaneous utilization of the link B_{util} at time T is averaged over an interval t and is given as follows:

$$B_{util}^{(T-t,T)} = \frac{1}{t}\int_{T-t}^{T} B(x)d(x). \tag{1}$$

Using this equation, the average available bandwidth over a time duration t can be computed as follows:

$$B_{avl} = \left(1 - B_{util}^{(T-t,T)}\right)C. \tag{2}$$

This further can be converted into percentage as follows:

$$\%B_{avl} = \frac{B_{avl}}{C \times 100}. \tag{3}$$

Interested readers are referred to [21] for more conceptual details of average available bandwidth, and its measurement and estimation techniques.

4.4 *Attack traffic modelling*

We assume that the attacker generates the attack flows from bots under its control using poisson distribution as a generating function at each bot. The attack rates generation function follows the poisson distribution, with rate of attack flow as a discrete random variable. Rate of flow has been considered as a random variable in the proposed mechanism, because of an uncertainty embedded in the assumption and analysis of attack rates. Poisson probability distribution of rate of attack flow r_i^a to be equal to threshold τ set by the proposed defence mechanism is given by the following equation.

$$P(r_i^a \simeq \tau) = \frac{\lambda^\tau e^{-\tau}}{\tau!} \tag{4}$$

where λ is mean value of rate of attack flows. Since the rate of attack flow r_i^a takes a discrete random value, its probability of acquiring a value less than or equal to threshold value τ can be computed using cumulative distribution function (CDF) of poisson probability distribution or the sum of all probabilities of $r_i^a \simeq \tau$ starting from 0 to τ using the following equation:

$$P(r_i^a \leq \tau) = \sum_{r_i^a=0}^{\tau} P(r_i^a \simeq \tau) \tag{5}$$

Equation 3 emphasizes the fact that the probability of the attack flow successfully reaching target server is also a ratio of fair share of bandwidth B allotted to it to the attack rate adopted by it [22]. To acquire more bandwidth, more attack flows need to have the attack rate less than or equal to the τ set by proposed defence mechanism. The ratio can be written as

$$ratio = \left(\frac{B}{r_i^a}\right). \tag{6}$$

5. Game formulation

5.1 *Players and their strategic space*

In this section, the proposed defence mechanism based on game theory is presented. The game is a two-player zero-sum game between an attacker and a defender. The first player is the defender, who has a clear knowledge of the capacity C of the link between the edge router and target server. The ABE tool is present in the link to obtain a value of average available bandwidth B_{avl} over a time interval Δt. The time interval Δt between two bandwidth checking times is based on the congestion occurrence at the link. Its value can vary from milliseconds to seconds. The defender decides a threshold value τ of rate per flow. It computes the payoff or utility obtained by choosing that value of τ as its strategy. If the utility by selecting such a value of τ is less than the utility obtained previously and congestion occurs, defender decides to choose new τ by checking B_{avl} again from ABE. If the utility is the same and no congestion has occurred at the link, the defender sticks to that value of τ

for some duration. If the utility by selecting τ is higher than the previous utility, the defender marks the current value of τ as an optimal strategy. Setting τ in such a way leads the game to a Nash equilibrium state. Some legitimate flows can also be dropped even at the optimized value of τ, but such trade-off analysis is done based on current utility and relative impact of the attack on legitimate flows. Defenders also want to learn more about the attack behaviour to maintain a knowledge database to classify a flow between an origin destination pair as a pure attack behaviour. Such flows having pure attack behaviour are straightaway dropped by edge router in future. To accomplish this, a flow has to be redirected to honeypot. For redirecting a flow to honeypot, defenders decide an upper threshold value $\tau\beta$. The flows having rates between τ and $\tau\beta$ are redirected to honeypot. Flows having $r^a > \tau\beta$ are dropped completely. The instantaneous value of threshold τ will be decided by the defender based on B_{avl} and total number of flows N at a particular time, given as follows:

$$\tau = \frac{C}{N}\left[1 - \frac{1}{\%B_{avl}}\right]. \tag{7}$$

Setting τ in such a way enforces equal and weighted fair share of bandwidth to every flow regardless of TCP/TCP-friendly or UDP flows. Decisions by the the defence mechanism are taken as follows:

- if $r_i^a \leq \tau$ let the i^{th} flow pass,
- if $\tau < r^{a_i} \leq \tau\beta$ redirect the i^{th} flow to honeypot,
- if $r_i^a > \tau\beta$ drop the i^{th} flow entirely,

where $\beta = 1.25$ is an adjustment value.

The second player of the game is an attacker who controls the botnet. The botnet size is denoted by S^{bot}. If S^{bot} equals 1, the attack is a simple DoS attack; otherwise it is a DDoS attack. The attacker wants to occupy maximum bandwidth of a link l to increase its utility. It can adopt two strategies. One is to increase the rate (r_i^a) per attack flow. It can increase the rate r_i^a by constant bit rate (CBR), in geometrical or exponential increasing manner. Increasing r_i^a has less implementation cost but has higher risk of dropping, detection or redirection of the attack flow to honeypot. Redirection of a flow to honeypot imposes a penalty cost γ in the total payoff obtained by the attacker. Penalty cost is justified because if the attacker is caught, its flow is purely classified as an attack flow and dropped entirely in future. The second strategy is to maximize the probability $P(r_i^a)$ of i^{th} attack flow to be less than the threshold τ. To do so, it has to lower its (r_i^a) per flow and simultaneously increase the S^{bot} under its control and split the flows among them with lower (r_i^a). Acquiring a bot involves a cost denoted by ω per bot. If its total cost is higher than total attack benefits, a rational attacker refrains from launching a DoS or DDoS attack.

5.2 *Modelling payoff functions*

The payoff function of attacker is to maximize an absolute impact on the network as a whole and simultaneously causing a relative impact on the legitimate flows [3]. The attacker's payoff function can be represented as follows:

$$U_a = \alpha\left(\frac{B_o^a}{C}\right) + (1-\alpha)\left(1 - \frac{B_o^l}{B_w^l}\right) - \omega S^{bot} - \gamma \tag{8}$$

where B_o^a is total bandwidth occupied by the attack flows m' that are able to pass and computed using Eq. (10). Value of m' is computed using Eq. (9). B_o^l is bandwidth occupied by the legitimate flows and B_w^l is the total bandwidth requirement of legitimate flows; α is a scaling factor used to balance the effect of absolute impact on bandwidth and relative impact on legitimate flows; ωS^{bot} is the total cost of maintaining the botnet size of S^{bot}; γ is the penalty cost inflicted upon attacker if a flow is classified as pure attack flows by the honeypot.

$$m' = mP(r_i^a \leq \tau). \tag{9}$$

Then

$$B_o^a = \sum_{i=1}^{m'}(r_i^a). \tag{10}$$

The payoff function of the defender is also designed in a similar way. Since the mechanism proposes a zero-sum game, the benefits of attacker are losses to defender and vice versa. Hence, defender's payoff function can be represented as the negative of the attacker's utility function as follows:

$$U_d = -\left[\alpha\left(\frac{B_o^a}{C}\right) + (1-\alpha)\left(1 - \frac{B_o^l}{B_w^l}\right) - \omega S^{bot} - \gamma\right]. \tag{11}$$

5.3 *Dominant strategies and Nash equilibrium analysis*

In the game presented earlier, the attacker adopts attack rate r_i^a for i^{th} flow per bot with a botnet size of S^{bot}. Attacker's total cost of maintaining the botnet is quantified as ωS^{bot} with an additional penalty cost of γ . The attacker needs to decide an optimal attack rate r^{a*} per flow per bot with an optimal botnet size S^{bot*}, so that U_a is maximized with minimum costs and minimum risk of dropping, detection or redirection to honeypot by edge router. On the other hand, to make the attack costlier, the defender needs to calculate an optimal value of threshold τ^* per flow so that maximum attack traffic can either be redirected to honeypot or dropped completely. This optimization problem can be solved in

a nonlinear manner by quantifying network parameters and attacker's incentives as described earlier, and the results can be represented by contour graphs. The game converges to Nash equilibrium and suggests the optimal strategies. No player is benefited by deviating from the optimal or Nash strategies. If a player deviates from the Nash strategies, it receives a lesser payoff. The Nash equilibrium strategies are denoted by the tuple S^{bot*}, r^{a*}, τ^* , which satisfy the following:

$$U_a(S^{bot*}, r^{a*}, \tau^*) \geq U_a(S^{bot}, r^a, \tau^*) \quad \forall \quad r^a, S^{bot}, \quad (12)$$

$$U_d(S_n^{bot*}, r^{a*}, \tau^*) \geq U_d(S_n^{bot*}, r^{a*}, \tau) \quad \forall \quad \tau. \quad (13)$$

6. Experimental results and discussion

MATLAB is used for numerical calculations and experimental purpose to suggest Nash equilibrium strategies for defending against DoS/DDoS attacks. The graphs generated using MATLAB show some interesting results and inferences that are in favour of the proposed defence mechanism, and advocate the worthiness of the work. For numerical computations, some initial values are taken as inputs to the game. Different flow rates of 10 legitimate nodes are taken in an array $n1$=[40, 45, 45, 40, 43, 35, 38, 39, 40, 45]. Attack flow rates of 10 attacker nodes or bots are taken in an array $m1$=[48, 58, 48, 60, 48, 68, 48, 62, 46, 64]. Hence the total number of flows N is 20. The link capacity C between the edge router and server is taken as 1000, with value of β equal to 1.25, α equal to 0.6, ω equal to 0.02 and γ as 0.0002. Initially, 100% bandwidth is available for transmission of flows. The results obtained are discussed as follows.

6.1 *Threshold setting by defender*

Based on the initial inputs and percentage of average available bandwidth at time t_0, the defender sets its threshold τ per flow, which is approximately equal to fair share of bandwidth allotted to a flow. The MATLAB calculation results in a graph as shown in figure 2 for setting τ as per average availability of bandwidth at a particular time t_0. The defender behaves aggressively when the average available bandwidth $\%B_{avl}$ is less than 6%, and lowers the threshold of rates per flow τ significantly up to 0.1 or the minimum possible value. The total number of flows and congestion checking time also play important roles in deciding the value of τ. When there is more than 6% of average available bandwidth, defender behaves leniently and sets the τ as maximum and equal to fair share of a flow. The whole idea ensures that the network is never saturated or congested at a given point of time and DoS/DDoS attacks are avoided.

6.2 *Probabilities of attack flows to pass, redirect and drop*

The numerical computation in MATLAB for calculating different probabilities of the given attack flows at different threshold values set by the defender results in the graph shown in figure 3. Following results can be deduced from the graph.

- The minimum probability of attack flows to pass is equal to 0 when τ is between 0 and 38. It starts increasing with further increase in τ, and reaches the maximum of 1 when $\tau = 58$.
- Similarly, the maximum probability of redirection is equal to 0.73 when τ is between 0 and 37. The probability of redirection decreases with an increase in

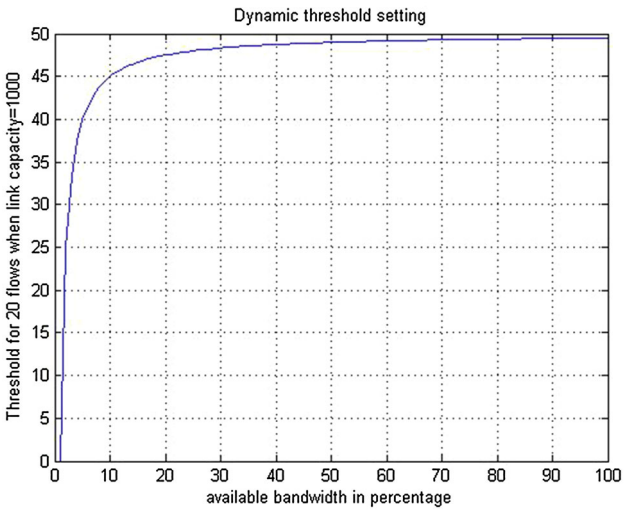

Figure 2. Dynamic threshold setting by defender.

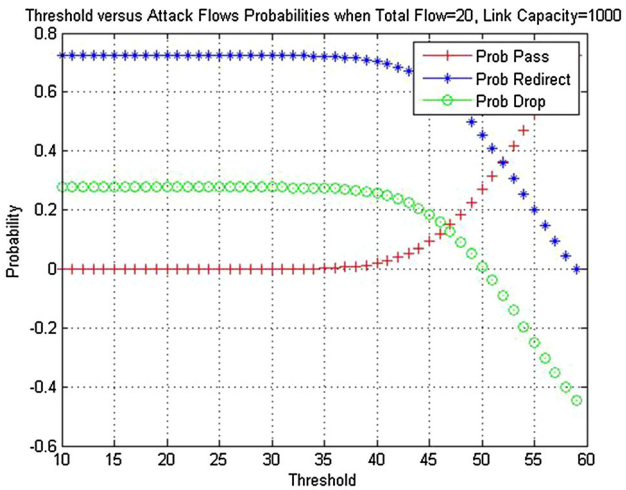

Figure 3. Attack flow probabilities.

the value of τ, and reaches the minimum of 0 when τ is set as 60 by the defender.

- The probability dropping of an attack flow is maximum when τ is between 0 and 35, which is equal to 0.27, and 0 when $\tau = 50$. The zero probability of dropping an attack flow is because of the defender setting an upper threshold $\tau\beta$, resulting in an upper value of τ equal to 62.5. No flow is dropped, but still some probability of redirection exists between τ 50 and τ 62.5.
- The attack flow probabilities to pass, redirection to honeypot and dropping at $\tau = 47.50$ are approximately equal to 0.20, 0.65 and 0.15, respectively. The utility of the attacker and defender in a game depends upon these probabilities. The attacker always tries to minimize the drop and redirection probabilities and maximize the pass probability of the attack flow. To do so, it shapes the traffic and sets the attack rate r^a per flow either equal to or less than τ while optimizing the botnet size and attack costs.

6.3 *Payoff of attacker and defender*

Equations (8) and (11) are computed in MATLAB with the initial inputs as discussed earlier. The results obtained are shown in figures 4 and 5. Following points can be deduced from the graphs.

- Payoff or utility of attacker remains positive, constant and equal to 0.2 when τ is between 0 and 37. This is because setting the value of τ in this range by the defender causes all normal and legitimate to drop, which is the ultimate goal of the attacker. Loss of legitimate flow is a benefit to the attacker, giving it a positive payoff. However, payoff or utility of attacker significantly decreases when τ is 37.5–40 and 40–43.5 subsequently. Utility of the attacker is minimum and equal to –0.25 approximately at $\tau = 47.5$. From the game theory point of view, $\tau = 47.5$ is the best response of the defender chosen in the game with given initial inputs.
- Utility of defender remains negative and constant, which is equal to –0.37 when τ is between 0 and 37. The negative sign indicates loss. The loss is due to dropping of some normal or legitimate flows. However, it significantly increases and reaches its maximum at $\tau = 47.5$. Subsequently, it again starts decreasing with increase in τ. From the game theory point of view, choosing a botnet size of 10 is the best response of the attacker with given attack rates, and choosing $\tau = 47.5$ is the best response of the defender. The defender adheres to the strategy of choosing $\tau = 47.5$, but the changes in inputs result in a new payoff and the defender needs to adjust to the changes.
- Now, if the best response of the defender is an optimal value of $\tau = 47.5$, the attacker sets the attack rates $r^a \leq 47.5$ per flow for launching the attack. It optimizes the size of botnet and attack rate per bot to maximize its payoff. From figure 5, it is construed that the utility or payoff of the attacker is maximum and equals 0.4205 on selecting total number of 12 flows or 12 bots with each having an attack rate equal to 43.18. The attacker adheres to this strategy as an optimal strategy.
- The tuple $S^{bot*} = 12$, $r^{a*} = 43.18$ and $\tau^* = 47.5$ are in Nash equilibrium for a given scenario at a particular stage of the game. An increase or decrease in botnet size increases or decrease the total number of the nodes. This affects the payoff of the defender and hence, it chooses to reset the value of τ again on the basis of utility and total number of nodes participating in transmission. A detailed study by employing multistage game can reveal more precise and accurate analysis of strategies of both players. However, we have left this as a future work.

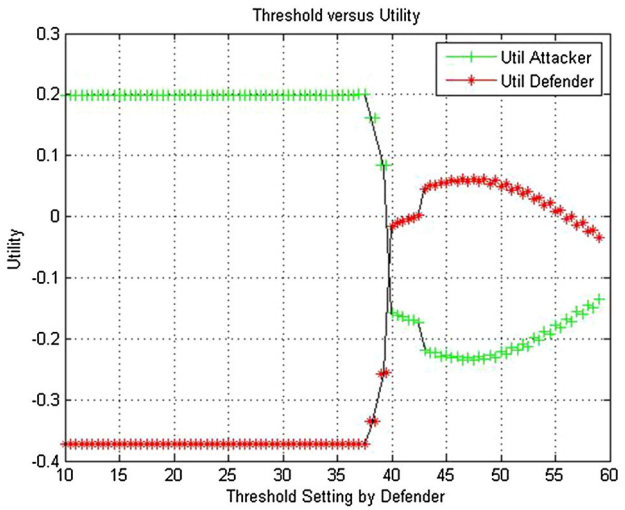

Figure 4. Utilities of both players.

7. Conclusion

In the era of complete dependency on networks for information communication, DoS or DDoS attacks pose a sever security threat to availability of network services round the clock. Several security measures are suggested to defend the networks against such attacks like traffic filtering, traffic shaping, trace-backing, validation or hybrid detection mechanisms, which place a computational or memory burden over networked devices and are not dynamically adaptive. The attackers are also more rational, incentives oriented, technically evolved and perform a cost–benefit analysis prior to launch a DoS/DDoS attack. These schemes neglect the designing of such incentives in modelling of defence mechanisms. This work proposes a game theoretical defence mechanism that addresses the issue of DDoS attacks

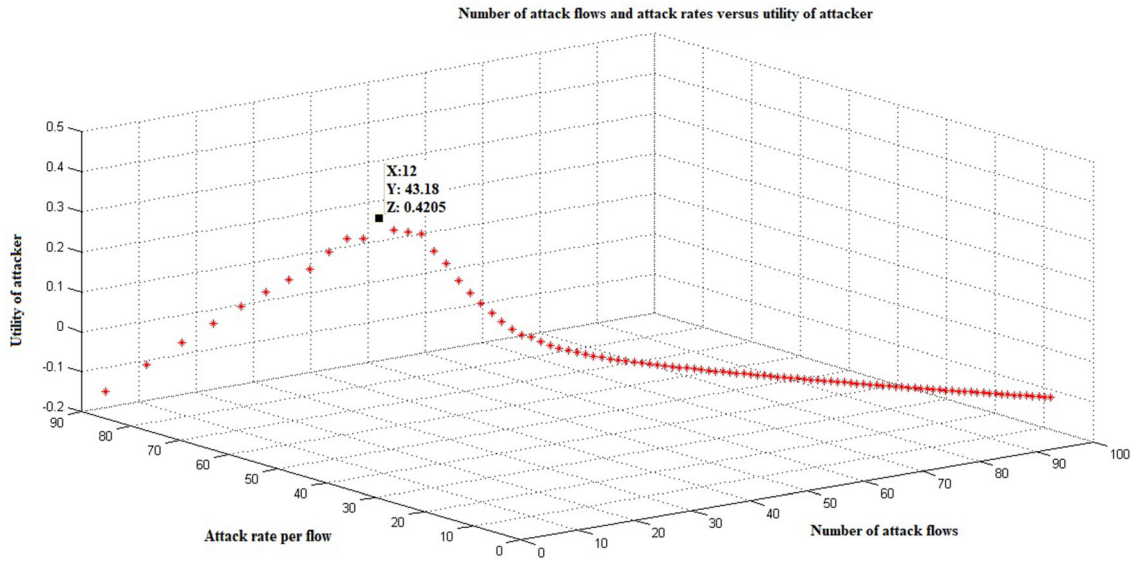

Figure 5. Utility of attacker when defender's best response is fixed.

based on bandwidth depletion by designing and quantifying incentives, and is dynamically adaptive to set an upper bound or threshold on network traffic to defend against DoS/DDoS attack. The methodologies and tools employed in launching DDoS attacks and current countermeasures against them are discussed. Limitations of current defence mechanisms are outlined. Attack traffic is modelled using poisson distribution. Average available bandwidth is estimated over an interval of interest. The proposed defence mechanism is based on zero-sum game. A finite subset of action space of attacker and defender is presented. Using the defence mechanism as a decision support system, the defender sets the threshold for a flow rate based on average available bandwidth estimated, total number of flows, capacity and utility of defender. Decisions to pass, drop or redirect a flow are taken based on the threshold set by the defender. Different probabilities of attack flows to pass, redirect or drop are calculated at the threshold. Based on these probabilities, cost and benefit analysis of the attacker is carried out. Corresponding to costs and benefits, the utility or payoff functions of attacker and defender are defined. Experiments and simulation are carried out using MATLAB. Nash equilibrium strategies of both players are derived based on the graphs generated. Thus, by choosing the Nash equilibrium strategy as suggested by the proposed defence mechanism for a given set of network parameters, a defender can attain an optimum level of network security round the clock and prevent or mitigate a DoS/DDoS attack.

8. Future work

The proposed work is based on pure strategy zero-sum game having a single stage. The results can further be refined using mixed strategy, dynamic and multi-stage games. The proposed defence mechanism can be embedded into a network router as a software code or can be implemented as a standalone device in network. This work has been registered as a project on Deterlab [23, 24] for verification and validation purpose in a more realistic scenario. Experimentations in NS-2 and Deterlab are under progress, and the results will be presented in future work.

References

[1] Zargar S T, Joshi J and Tipper D 2013 A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys and Tutorials* 15: 2046–2069

[2] Mircovik J and Reither P 2004 A taxonomy of DDoS attack and DDoS defense mechanism. *ACM SIGCOMM Computer Communication Review* 34: 39–53

[3] Liu P, Zang W and Yu M 2005 Incentive-based modelling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security (TISSEC)* 8: 78–118

[4] Manshaei M H, Zhu Q, Alpcan T, Basar T and Hubaux J P 2011 Game theory meets network security and privacy. *ACM Computing Surveys* 45: 25–25

[5] Bedi H S, Roy S and Shiva S 2011 Game theory based defense mechanism against DDoS attacks on TCP/TCP IP friendly flow. In: *Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*, pp. 129–136

[6] Osborne M J 2004 *An introduction to game theory*. Oxford University Press, Inc. 198 Madison Avenue, New York, 10016 https:////www.oup-usa.org

[7] Yaar A, Perrig A and Song D 2004 SIFF: Stateless Internet Flow Filter to mitigate DDoS flooding attack. In: *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 130–143

[8] Xu J and Lee W 2003 Sustaining availability of web services under distributed denial of service attack. *IEEE Transactions on Computers* 52(2): 195–208

[9] He W, Xia C, Wang H, Zheng C and Ji Y 2008 A game theoretical attack defense model oriented to network security risk assessment. In: *Proceedings of the International Conference on Computer Science and Software Engineering*, pp. 498–504

[10] Alpcan T and Sonja B 2011 Security games for vehicular networks. *IEEE Transactions on Mobile Computing* 10: 280–290

[11] Zhu Q, Li H, Han Z and Basar T 2010 A stochastic game model for jamming in multi channel cognitive radio systems. In: *IEEE Proceedings of the International Conference on Communications (ICC)*, pp. 1–6

[12] Kiekintveld C, Lisý V and Píbil R 2015 Game theoretic foundations for the strategic use of honeypots in network security. In: *Cyber Warfare*. Cham: Springer, pp. 81–101

[13] Durkota K, Kiekintveld C and Bosansky B 2015 Game theoretic algorithms for optimal network security hardening using attack graphs. In: *Proceedings of the 14th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pp. 1773–1774

[14] Garnaev A, Baykal-Gursoy M and Poor H V 2016 A game theoretic analysis of secret and reliable communication with active and passive adversarial modes. *IEEE Transactions on Wireless Communications* 15: 2155–2163 https://doi.org/10.1109/TWC.2015.2498934

[15] Yang J, Kim I M and Kim D I 2013 Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers. *IEEE Transactions on Wireless Communications* 12: 2840–2852

[16] Zhang N, Lu N, Cheng N, Mark J W and Shen X 2013 Cooperative spectrum access towards secure information transfer for CRNS. *IEEE Journal on Selected Areas in Communications* 31: 2453–2464

[17] Zheng G, Choo L and Wong K 2011 Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Transactions on Signal Processing* 59: 1317–1322

[18] Paramasivan B, John M, Prakash V and Kaliappan M 2015 Development of a secure routing protocol using game theory in mobile ad hoc networks. *Journal of Communication and Networks* 17: 75–80

[19] Abegunde J, Xio H and Spring J 2015 Resilient tit for tat (RTFT): a game solution for wireless misbehaviour. In: *Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 904–909

[20] Prasad R, Constantinos D, Margaret M and Claffy K C 2003 Bandwidth estimation: metrics, measurement techniques, and tools. *IEEE Network* 17: 27–35

[21] Antoniades D, Manos A, Papadogiannakis A, Evangelos P M and Constantine D 2006 Available bandwidth measurement as simple as running wget. In: *Proceedings of the Passive and Active Measurement Conference (PAM)*, pp. 61–70

[22] Moti G, Herzberg A and Gev Y 2014 Bandwidth distributed denial of service: attacks and defenses. *IEEE Security and Privacy* 12: 54–61

[23] Mirkovic J and Terry B 2012 Teaching cyber security with DeterLab. *IEEE Security and Privacy* 10: 73–76 https://www.isi.deterlab.net/index.php3

[24] Mirkovic J, Fahmy S, Reiher P and Roshan K T 2009 How to test DoS defenses. In: *Proceedings of the Conference on Homeland Security (CATCH'09), Cybersecurity Applications and Technology*, pp. 103–111