Journal of Information Technology Research
Volume 13 • Issue 1 • January-March 2020

Taxonomy of Payment Structures and Economic Incentive Schemes in Internet

Brij B. Gupta, National Institute of Technology, Kurukshetra, India

Prachi Gulihar, National Institute of Technology, Kurukshetra, India

ABSTRACT

Recently the study of economics of internet has emerged as an emerging field of study. The workstations being distributed across the network along with the users having varied interests has made this study very important from an information security and policy designing point of view. The main purpose of any framework design is to keep up with the security standards of confidentiality, integrity and availability without being an overburden on the deployer. The same goes for the users, the Quality of Service (QoS) should be in accordance with what they pay for. The concept of "tragedy of commons" plays an important role in distributing the limited resources of the internet. In this, the users because of their own self-interest destroy the collective interest of a community sharing the resource. A sustainable pricing strategy is the one which is able to cater to the competitive advantage of different network providers offering the same set of services but on varied prices. A pricing mechanism will help in differentiating the services offered to the users, but another important task is of fixing the incentives. The pricing strategy plays a very important role in facilitating varied kinds of QoS requirements. Security professionals have realized that while designing any security mechanism it is vital to keep in consideration the "theory of mind" which explains the way the attackers and benign users take decision to deceive of remain loyal to the system. So, studying the incentive and payment structure from economic point of view is important.

KEYWORDS

Economic Incentives, Internet Economics, Payment Structures, Quality Of Service (QoS), Third-party Schemes

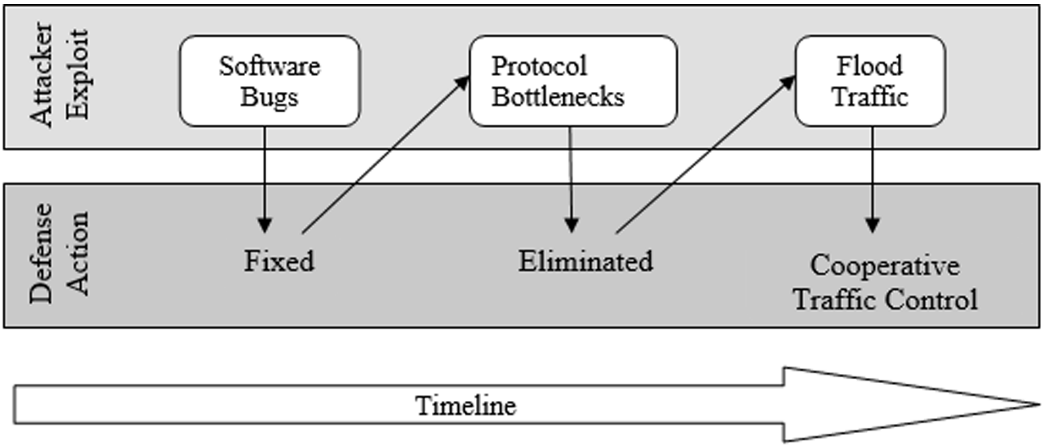
INTRODUCTION

A network is not owned by any single entity; its various parts may be under the control of different network providers. Whenever a data stream has to be sent from a sender to receiver then it has to cross the physical infrastructure of several owners. So, a global standardized pricing fails to create any sort of agreement among the organizations possessing traffic right of different places. This is an important research problem (Gupta, Stahl, & Whinston, 1999). Although designing such economic solutions in today's era of fast paced technology driven world is a cumbersome task but using the economic theories for the same will surely provide valuable support.

The level of Quality of Service (QoS) requirements expected by the users depend majorly on the kind of service want to be offered like high download speeds, quality of video and audio etc. This QoS level is described by three attributes- packet loss, bandwidth and delay. The QoS is application based which means that the scenario differences according to the application. E-mail service does not expect correct order delivery of packets, all it wants is that the message should be delivered without any loss of data whereas in the case of gaming applications the correct ordered delivery of packets is

DOI: 10.4018/JITR.2020010110

Figure 1. Evolution of DDoS attacks



necessary to maintain a consistent flow of audio and video. The QoS depends on the context of use by customers like although the ordered delivery of packets is not the requirement of e-mail service but the instant notification on arrival of any email is to be ensured. It also depends on the urgency of the task like instant download of files versus delayed download of files, for instant download the bandwidth availability must be enhanced and there is a constant variation in the quantity of packets being transmitted over a channel. So the pricing mechanism must be designed in accordance with the traffic generated. This needs to be accompanied by a fixed slab charge to ensure that enough revenue is generated to keep the services running.

The provision of incentives is necessary to prevent users from behaving dishonestly. The users should not be lured to the idea of masking their email message as a multimedia message to gain a higher priority on the network. Such tasks should be discouraged. This explains the need of pricing policies and incentives. Figure 1 explains the evolution of DDoS attacks over time (Adat et al., 2018; Gupta et al., 2016; Chhabra et al., 2013; Negi et al., 2013; Alomari et al., 2012). It depicts the need of incentive mechanisms in cooperative schemes. The current strategy for defense demands collaboration among defenders which is the motivation to design a fair policy scheme. Among many parameters on which the network performance depends, the main game-changer has been the resource allocation (Bailey, 1997). Application of concepts of economics will certainly help in improving the management of network. This is a lesser-explored field which will combine basics of economics and computer networks. For allocation of resources either the limits can be put on the quantity of the resource used or some pricing strategy can be defined if the user wants more resources than the allocated quantity. Putting a limit on the quantity of resources allocated requires a central authority to monitor the same. Although the advantage being lesser accounting costs.

In the pricing strategy, the users themselves get to choose the quantity for which they are willing to pay at the offered prices. Although this is a decentralized solution, but this leads to increased accounting costs because the amount of usage needs to be metered. But it is still a better strategy because a central authority is difficult to maintain on a global network and are always prone to single point of failure so a distributed solution is more preferred. The goal of economic pricing is to manage the resources available on the network to provide improved services to the users. Different kinds of users have different Quality of Service (QoS) requirements depending on their demands. For example, if a user wants to do video conferencing on the network then the network must be able to ensure synchronization and coordination in picture and sound. The network should also be able to cater to transfer of high volume of data with a high speed. This kind of variation in user requirements leads to the demand of a pricing mechanism which works efficiently in a distributed environment. This work explains the payment structures of Internet in the next section followed by different incentive schemes which motivates the peer nodes to collaborate and defend.

The reasons for failure of security in any system are two-fold. First is the poor design and second is the poor incentive. Although the design part has been widely explored but the incentive part remains naïve. Computer systems are failing because the group of people responsible to protect them does not suffer from complete setbacks on failure. Just as the mathematics concepts came as a boon for security industry in the form of cryptography 25 years back the same goes for theory of microeconomics now. The problem of incentives being misaligned has led to several frauds in the banking industry (Anderson, 1994). Construction and development of systems that promote fair behavior among the users is a must to maintain the security standards and lower the system failure rates. The innovative concept of online auctions as a reputation system has motivated the researchers to explore more such options. This feedback mechanism gave a vent to the free riding problem faced by eBay (Dellaracos, 2001). A striking example of economic analysis was shown in January 2005 when the power of online music sharing shifted from music vendors to individual publishers (Varian, 2015).

TAXONOMY OF PAYMENT STRUCTURES IN INTERNET

IP Packet Based Pricing

Huang et al. in (2007) have discussed usage-based pricing and proposed new market mechanism like Capacity Provision Network (CPN), Internet mapping, overlay networks. In usage-based pricing mechanism the user has to pay in accordance with the volume of traffic or data consumed. It is further of two types: IP packet-based and congestion based. In IP packet-based pricing the cost of one IP packet is fixed and in congestion based the cost of transmission of IP packet depends on the current level of congestion in the network. The only limitation of this is that the attack traffic must be large enough to provide enough incentives to ISPs to set up filters.

Capacity Provision Network (CPN)

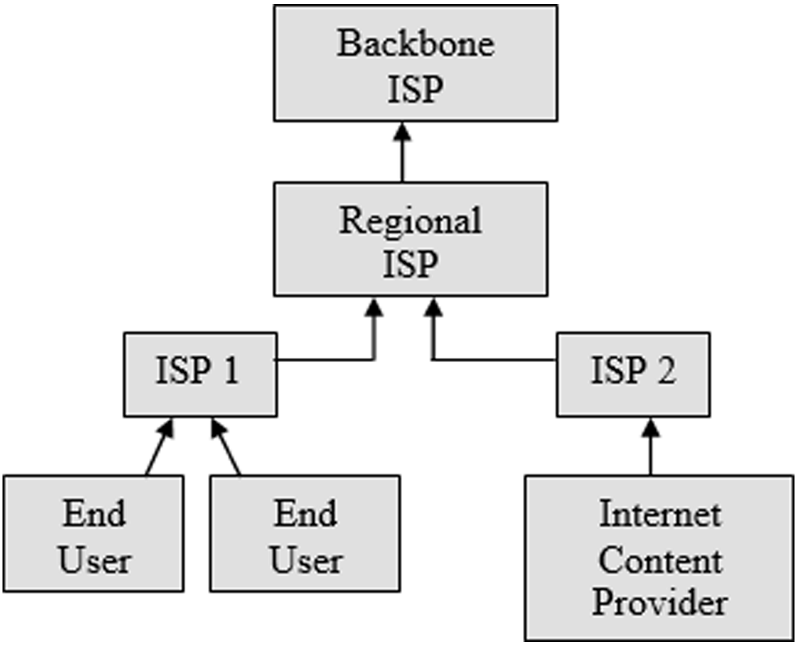
In CPN technique the concept of cache trading is used, which means that sending the overloaded attack traffic to ISP caches which are free in terms of space. All ISPs have cache servers to store frequently accessed pages, but these servers are not always full so sharing this capacity increases the total welfare. They have discussed two other technologies to ensure incremental payment structure in the internet- overlay networks and internet mapping. Removal of the limitation of signing multiple bilateral contracts for cache trading a CPN is proposed (Geng et al., 2002). Such a network fulfills the role of an intermediary between the different cache traders. To begin cache trading, the ISPs do not have to put extra investment. To create incentives they have deployed static structures of payment. Figure 2 depicts the flow of incentives in the internet.

The application of both these techniques- cooperative filtering and cooperative caching ensures that the traffic load is both reduced and distributed to other links preventing successful DDoS attack. The free cache will behave as buffer across the network. Using buffers on the output links will prevent the excess packets from getting dropped. These packets can be stored in these caches and can be examined for malicious traits post the attack. Although this is not an offensive approach but studying these packet characteristics will help the victim to analyze the practices of the attacker machine and hence improve its defense strategy.

Overlay Networks

An overlay network is a content intermediary usually seen in the entertainment websites which ask for additional payments to use their services like downloading music, movies or buy some subscriptions. They are basically application level networks which are based on the existing infrastructure of the internet. Multiple overlay networks provide independent services, but they share internet resources like network bandwidth for communication.

Figure 2. Chain of incentives in internet



Internet Mapping

Another technology to ensure incremental pay structure is internet mapping. Internet mapping is an approximation of the delay between two cooperating nodes in the internet depending on their location and distance between each other. This technique has two main drawbacks. Firstly, there may be instances where the cache server in best position to cooperate may cheat and respond with its wrong location position because it does not wish to cooperate due to low incentives. Secondly, the cache server in best position to help may be engaged in other activities so this dynamic scope of change in activities need to be considered for its practical use. Table 1 consolidates all these schemes.

Externality Based Scheme

The basis for any economic pricing strategy on any network is that the pricing mechanism should be incremental. This means that all the entities which comes in the path from sender to receiver needs to be economically incentivized. Here the concept of externality pricing is more prevalent. In this kind of policy, the incentives charged will depend on other services competing for the bandwidth at that point of time.

Like, the price to send a video clip from point A to point B in the network will vary in accordance with the amount of delay this sending task is going to cause in other services on that network path. This is the reason why internet services are cheap during some hours of the day and the rates increase during the peak working hours. Same is the reason behind cheaper call rates during the night time. But the problem of pricing is more complex when it comes to resource allocation. So, in the pricing mechanism there will be a fixed charge to cover the costs incurred in providing services and an additional charge is imposed according to the externality principle. This ensures that the user who is in the utmost need of the resource bids the highest for getting access to it. The resource in this may be bandwidth, cache, computing power etc.

Table 1. Payment structures in internet

Name of scheme	Author	Scheme description	Limitations
Capacity provision network (2005)	X. Geng et al.	Network of cache servers is owned, operated and coordinated through capacity trading	Signing bilateral contracts with each of the cooperating nodes too costly to be practical
Overlay networks (1994)	J. O. Ladyard, K. S-Moore	Beside the payment to ISPs, each user pays fees to utilize a specific Internet services	• Discrepancy in fee structures among various overlay networks • Possibility of free riding
Internet mapping (2002)	T. S. E. Ng, H. Zhang	Incentives offered based on the positions of several reference nodes and delay to each of them	Only effective when the participating nodes are truthfully report their locations and delay information
Barter based (2004)	Kostas G Anagnostakis et al.	Enforce repeated transactions in a small subset of the network	Works only in a small network with high footprint

Congestion Based Scheme

Another kind of pricing mechanism is dynamic which is depicted in figure 3. In this the prices offered depends on the level of congestion in the network. More the congestion levels, more is the price charged to transfer packets via that route. This can be explained by a spiral diagram as below. The lower priority traffic remains in the outermost circle and the highest priority traffic resides in the innermost circle. The service begins from the innermost circle then it is offered to the outer circles. This way multiple services are segregated according to their priorities. And the priority is decided by the amount one pays for using the service or resource. For the services offered in the external circle only the fixed fee is charged whereas usage-based prices are charged for the services offered in internal circle.

Cooperative Filtering and Caching

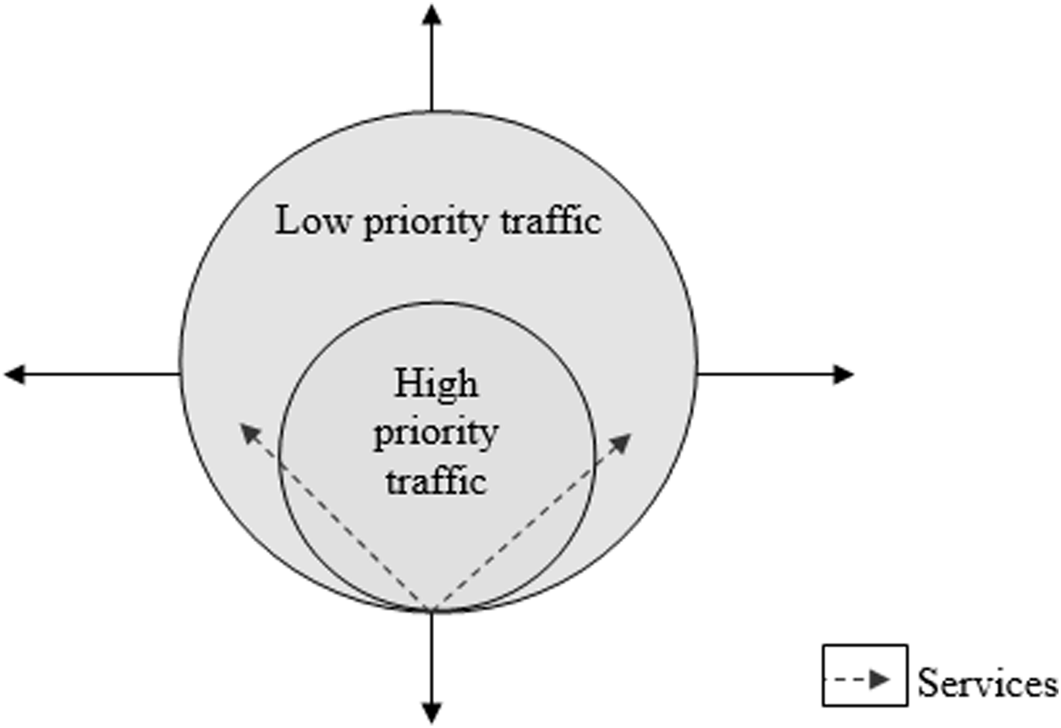
Two types of cooperative techniques exist- cooperative filtering (Solman, 1994) and cooperative caching (Geng & Whinston, 2000). In cooperative filtering, the ISPs which are in the way of the attacker's path filter out the malicious traffic in cooperation. And in cooperative caching, instead of filtering the malicious traffic the whole set of traffic is diverted to several ISP caches. Local defense point faisl miserably when the DDoS flood attacks the entry router of the network. So just by having security control systems on its own boundary, the victim cannot prevent DDoS attack. The traffic control systems are effective only when the defense is done in collaboration with other prospective victim nodes.

The cooperative filtering solution first generates an alarm indicating some malicious activities. This is done using an Intrusion Detection System (IDS) which is responsible to do a pattern analysis of the incoming packets and then sending alarm messages on detection of malicious traffic. After spreading of alarm messages, it traces back the traffic to find out the source of traffic generation. The filters along the path traced back are activated and they begin filtering. The attacker machine's ISP will be informed of the malicious activity which will then make the machine go offline. This is possible only when the source machine is traced back successfully, which is a very difficult task. Lastly, it begins filtering out the malicious traffic.

Joint Allocation

For joint deployment of cooperative filtering and cooperative caching, joint allocation of resources (Elwalid et al., 1995) must be done. The below figure 4 explains the manner in which the caches are arranged in the internet. Whenever the local ISP cache is overloaded it seeks cooperation from

Figure 3. Services distribution

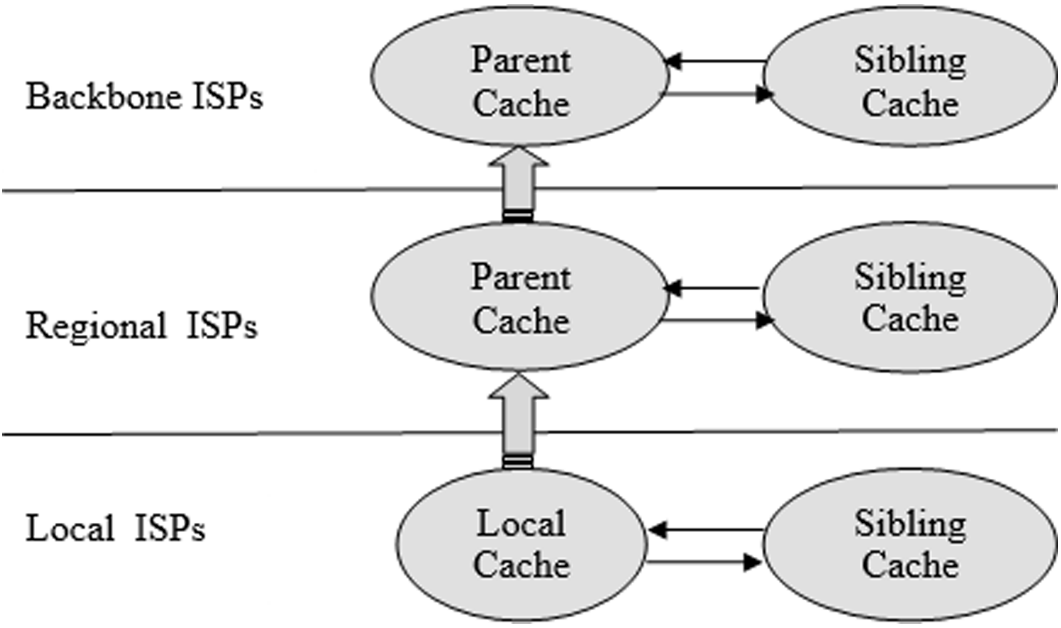


the sibling cache and when all the sibling cache resources are exhausted, then caches higher up in the hierarchy are approached for cooperation. Allocation of resources must be fair due to many reasons. Firstly, the fair allocation of resources eliminates the bottlenecks in the network improves the performance. Fair allocation guarantees fulfillment of QoS requirements. Even if the network may not get congested, but fair allocation ensures that the traffic streams are isolated. Fair allocation of resources is a countermeasure to prevent DDoS attacks because if the allocation is not fair then the resource may be used excessively which is one way how DDoS attack takes place, by exhausting the resources. Three kind of fairness notions exist for resource allocation – max-min, utility max-min and proportional max-min.

1. Max-Min Fairness- In max-min fairness scheme (Keshav, 1997), the nodes demanding the resource have equal rights to demand the resource and the resource is allocated according to the demand in increasing order.

2. Utility Max-Min Fairness- In utility max-min (Cao et al., 1999), the allocation of resource is dependent on a utility function. The basis for any policy design is based on utility max-min fairness scheme. The utility function varies under different traffic circumstances like real time traffic or adaptive traffic.
3. Proportional Fairness- The drawback of both these schemes is that a greater priority is given to the node with lesser demands. To overcome this drawback, the proportional fairness scheme (Kelly, 1997) is discussed which never over allocates the resources to the nodes with smaller demands. It maintains an allocation vector to keep over allocation of resources in check.

Figure 4. Hierarchy of caches in the internet



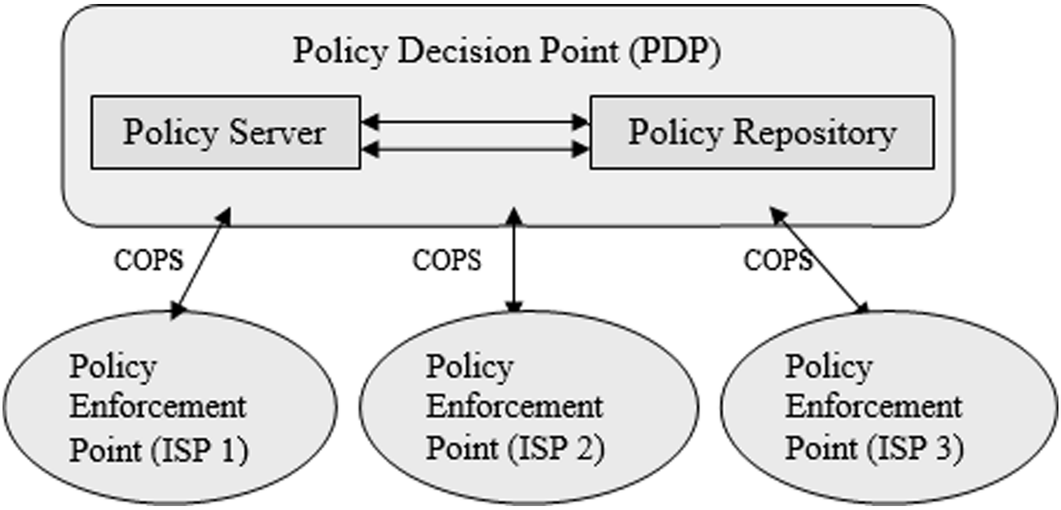
Policy Based Networking (PBN)

For implementation of the usage based-policy we use of the technology of PBN is made. This is a representative implementation scheme which addresses cost-effectiveness of the designed policy (Yavatkar & Pendarakis, 2000). The aim is to enhance the development of infrastructure of internet as a more secure platform by preventing DDoS attacks. For the successful implementation of any usage based scheme the ability of the network to manage the traffic plays a very important role because of existence of cross-border attacks. The above designed policy is implemented using the PBN framework as follows. The rules setting the actions to be taken under different circumstances are defined. These rules are specified in the form of policies which will control the resources of any system, in this case the ISP cache and bandwidth of the network. There are two parts of the PBN framework- Policy Enforcement Point (PEP) and Policy Decision Point (PDP). From the perspective of PBN the Directory Manager will be the PDP. And the participating ISPs become the PEPs. The PDPs and PEPs exchange the information of their policies through a Common Open Policy Service (COPS) protocol (Boyle et al., 2000).

Various kinds of policies can be implemented using PBN. Firstly, the policies which are defined by the cooperative ISPs and cannot be altered by the receiver ISPs. For example, increasing the level of performance by restricting the entry of traffic using admission control in data link layer. This ensures traffic is controlled even if the in-path devices are compromised. Secondly, the ones defined by the victim ISP which cannot be changed by the cooperative ISPs. For example, assigning a cap limit to the traffic being transferred and generating an alarm if the diverted traffic exceeds the cap limit. This means that the amount of malicious traffic has become uncontrollable and some other caches are needed for diversion.

For both of these, special hardware requirements must be met. Another kind of policies, software policies can also be defined in PBN. Software policies help to achieve multiple levels of security (Das et al., 2000). The TCP/IP gateways behave as proxy policies. Defining policy rules for these proxies, they can be made to filter out the traffic in cooperation and similarly policies for dynamic pricing can

Figure 5. Architecture of policy based networking


Policy Decision Point (PDP)
Policy Server
Policy Repository
COPS
COPS
COPS
Policy Enforcement Point (ISP 1)
Policy Enforcement Point (ISP 2)
Policy Enforcement Point (ISP 3)

be defined on the basis of usage. A coordinated network is formed globally with the help of PEPs which will help in minimizing DDoS threats. Figure 5 shows the architecture of policy-based networking.

TAXONOMY OF ECONOMIC INCENTIVE SCHEMES

In this portion various prevailing incentive scheme mechanisms and their limitations are discussed. Sometimes there exists a lack of incentive mechanisms in systems and at other rimes the incentives provided are not enough for the cooperative nodes to share the resources. First we discuss the various incentive mechanisms then we discuss some reengineered market mechanisms offering better economic structures and policies.

Reputation System

A reputation-based system (Mousa et al., 2015) in which the participant's behaviour is considered to as a measure of honesty. Use of the system of participatory sensing is made which is based on the rating and feedback of the participating users the node is given a rating or score. Participatory sensing makes use of camera, Global Positioning System (GPS) and various sensors and its use can be widely seen in traffic monitoring, sports monitoring, weather monitoring and online shopping. The devices are embedded with Trusted Platform Module (TPM) which ensures the authenticity of the participating nodes.

The reputation-based systems are vulnerable to numerous attacks namely corruption attack, on-off attack, re-entry attack, collusion attack, Sybil attacks, GPS spoofing. These were the direct attacks. A set of indirect attacks affecting the ratings are also possible namely badmouthing attack, ballot stuffing attack and unfair ratings.

Tit-For-Tat System

A barter based tit-for-tat scheme (Mei & Stefa, 2012) is the one in which they have dealt with the fundamental question of why would the intermediate nodes will spend their own energy and bandwidth to carry messages for other nodes. They introduced two packet forwarding mechanisms- GiveToGet (G2G) Epidemic Forwarding and

Table 2. Economic incentive mechanisms

Name of scheme	Author	Scheme description	Limitations
Reputation system (2015)	H. Mousa et al.	Scores are given to nodes on behaving honestly	● Vulnerable to collusion attacks, sybil attacks and whitewashing attacks. ● Vulnerable to coordinated gaming strategies due to distributed rating systems
Tit-for-tat (2012)	A. Mei, J. Stefa	Mobile user cooperate on the principle of double coincidence of wants	● Restricted to applications with long session duration ● Hard to meet different service requirements of the user
Credit based (2016)	Y. Wang, Z. Cia, G. Yin, Y. Gao	Peers earn currency by contributing resources to the system	● Rely on central authorities ● No explicit provably secure digital currency system used
Usage based (1999)	A. Gupta et al.	Ties payments to actual traffic volumes	Fails when the attack traffic is not large enough to cause congestion

G2G Delegate Forwarding. Although other mechanisms rely on altruistic cooperation of nodes these two mechanisms are robust to different distribution of altruism of nodes thus preventing selfish mining. In G2G Epidemic Forwarding every contact is used to forward the message due to which overhead in terms of multiple copies of the same message exists.

In G2G Delegation Forwarding a forwarding quality is associated with each node and forwarding of the message depends on the node the message is destined for. They are based on the concept of double coincidence of wants in which an equal amount of services are exchanged but the drawback such scheme is that two nodes need to remain in contact for long durations so that several cycles of exchange can take place hence nullifying the burden on either of the nodes in cooperation.

Credit Based System

A credit-based system (Li et al., 2016) which is resistant to collusion attacks. In credit-based systems there is a central authority which distributes some currency the nodes in the network, then these nodes can cooperate and share the resources with each other by the exchange of this currency. This currency may be a fiat currency, or digital currency like e-cash and virtual money services. We will be addressing a major drawback of this scheme which is reliance on central authority due to absence of provable secure digital currency. Due to presence of central authority these schemes cannot be applied in Peer-to-Peer (P2P) network applications. They have proposed an auction model in which several the economic properties like individual-rationality, incentive-compatibility, efficiency, optimality and budget balance are considered. Table 2 consolidates some of the discussed economic incentive mechanisms.

Flat Rate Pricing

All the various usage-based pricing schemes adopted over the internet can be broadly classified into two types- flat rate and usage based. Although the flat rate schemes are easier to implement but they are unfair for users demanding different QoS. The usage-based schemes increase the fairness level but with the involvement of complex billing systems. The payment structure existing on the internet do not support effective cooperation among different participants. The policy of a fixed subscription fee is most prevalent payment structure.

But this does not consider the actual amount of data being used because of which came the usage-based fee structure. An optimization needs to be set up between the cost and benefits of any scheme. The counting of packets in the internet is a costly task, so the usage-based pricing schemes do not base themselves solely on traffic pricing but mainly on resources like cache and bandwidth used.

Real Time Usage Based

In (Gupta et al., 1996) a computational approach is suggested to calculate this usage-based fees in real-time. The approach makes use of parameters at individual nodes instead of network wide parameters. On simulation of this approach on about 100 nodes, the results found the dynamic approach based on congestion level to be better than both fixed and externality-based approaches of traffic pricing. This brings us to think about which characteristics affect the viability of any pricing mechanism on internet. The usage based pricing schemes help the network providers in fairly recovering the costs of the services provided.

Any single pricing strategy is not sustainable in internet so in (Gupta et al., 1995) are discussed some characteristics which must be kept in mind while designing any economic solution. For participants to continue participating in pooling their resources, the fundamental concept is that the Return on Investment (ROI) should be greater. The valuation of ROI varies drastically due to absence of any set standards to calculate it. The fixed price incentive mechanisms are not adaptable to changes in the network conditions. This is why dynamic incentive mechanism is preferred.

Usage based pricing is widely found in data, cloud storage and payment services. Data services use usage-based pricing for paying for data utilized. Cloud storage uses usage-based pricing to charge for the storage space being provided. And the payment services use it to charge for processing a transaction in the payment procedure. Usage-based pricing is also known as Pay As You Go strategy. In this the user is either charged in advance or later in the form of arrears. This kind of scheme motivates to optimize the resource utilization because the whole strategy is money driven. The advanced strategy works like the credit card system and the arrear one works like the month-end utility bills of water, electricity etc. The policy is generally divided into two parts- resource allocation and pricing strategy. The analysis of any policy from a brokering point of view is very essential.

Dynamic Bidding Auction

In the dynamic incentive mechanism, the participating entity rents out its resources for a duration of time against the offered bid prices. There are many advantages of a dynamic pricing policy (Bichler, 2001) like quick adaptation to the network condition. The problem of starvation of participants having higher evaluation of their resources exist, but this problem has been resolved in (Lee et al., 2010) by offering participating incentives to the entities who lose in the bidding auction. This promotes more entities to take part in cooperation and the active life cycle of any bidder multi-folds thus preventing any shoots in prices due to a competitive network set-up.

RELATED WORK

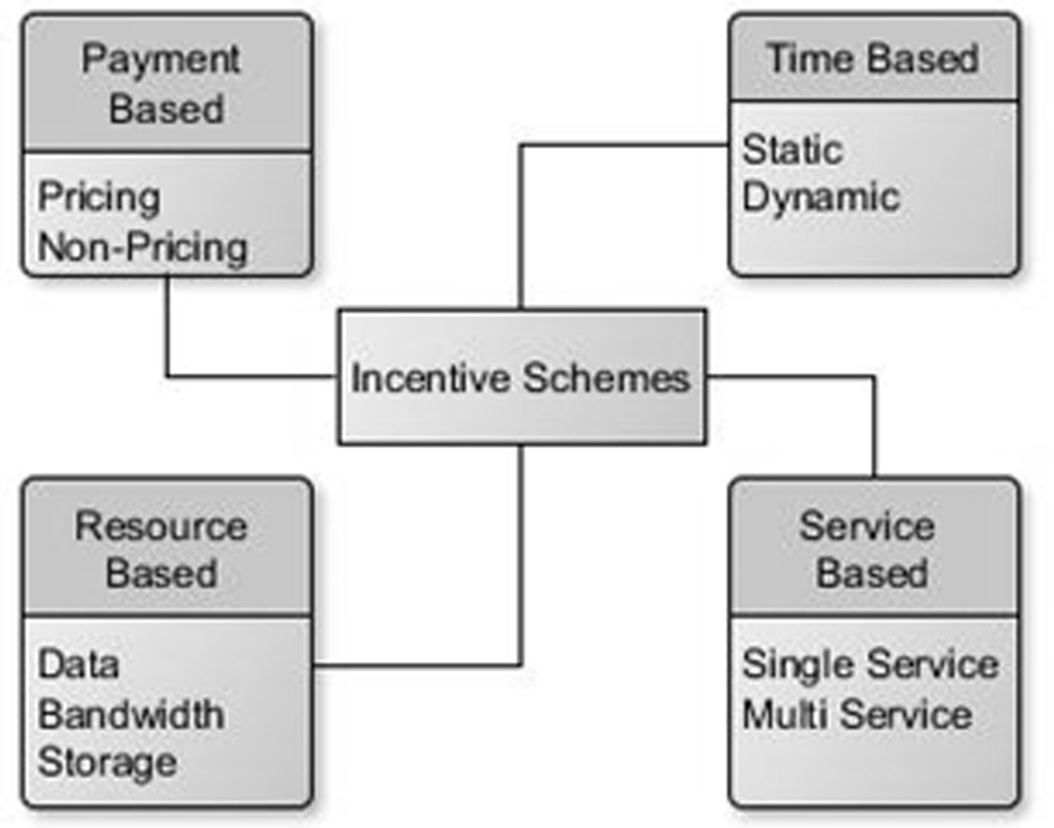
In the third-party detection the victim depends on some third party which handles the DDoS attack risk for economic incentives. The third party is responsible to detect the DDoS attack and signal the victims and it is the third party only which is responsible to counteract by taking defense measures against the attacker.

The victim has to compensate the third party by paying for the services it offers. Here comes the role of the economic solutions defending different cyberattacks. The classification of the various incentive schemes used is shown in figure 6.

Dawn et al. (2001) have discussed the IP traceback problem in which the attacker is unable to be identified because he makes use of spoofed IP address to launch the DDoS attack. They discuss two schemes based on the concept of packet marking. One is the advanced packet marking scheme and the other is the authenticated marking schemes which support incremental deployment and the victim node is able to traceback the attacker's path when the attack is performed.

They make use of edge sampling algorithm for packet marking but instead of appending the additional data onto the packets it has overloaded the 16-bit IP identification field. In their encoding

Figure 6. Classification of incentive schemes



scheme they have divided this 16-bit field into two parts- 5-bit distance field and 11-bit edge field which is further extended by using two independent hash functions. The authenticated marking scheme prevents the compromised routers from forging the router markings by authenticating them by using only one cryptographic Message Authentication Code (MAC) marking instead of digital signatures which are expensive to compute and have large storage overheads.

Andrey et al. (2003) proposed an IP traceback mechanism with Deterministic Packet Marking (DPM). Although this approach is effective only when the attack traffic is small, but the main advantage of this scheme is that the service provider can implement this without revealing its internal network structure and without any additional processing overheads. DPM has been successful in addressing the limitations of Probabilistic Packet Marking (PPM) technique but this work has assumed that all the ISPs will engage in DPM which is an unrealistic assumption. It has been designed by considering interfaces as the units of traceback instead of routers as units of traceback. Every packet is deterministically marked when it enters the network, this marked remains static till the packet is in the network. When attacker tries to spoof the mark then the spoofed mark is overwritten by the correct mark on the next hop of an honest router.

Drew et al. (2002) have proposed an algebraic approach to IP traceback problem. They have catered to this problem by considering IP traceback a polynomial reconstruction problem and by using algebraic techniques to solve it. It is also incrementally deployed scheme which embeds the router information randomly onto the packets and then encodes them as points on the polynomial which are then reconstructed at the victim node. This scheme is not only limited to DDoS attacks but is also actively used in congestion control, routing and configuration management of the network statistics. It proposes two algorithms-algebraic edge encoding and algebraic full path encoding using Vandermode matrix, but the issue is that output number of bits are too large to be accommodated in a single IP packet.

Savage et al. (2001) proposed a network support scheme for IP traceback based on marking the packets in a probabilistic manner. They have proposed two algorithms- node append algorithm and node sampling algorithm. Node append algorithm simply appends the address of the node at the end of the packet as it crosses different nodes from source to destination. The node sampling algorithm samples one node at a time instead of the full path which reduces the router overhead and space requirements. But there are two major limitations in this approach. Firstly, finding out the order of the router from the sampled collection is not possible and secondly, if the attackers are multiple in numbers then there may arise a condition where multiple routers exist at the same distance from the victim so the sampling technique will fail to collect distinct data.

Snoren et al. (2001) suggested a hash-based IP traceback mechanism. They draw attention of the researchers to the issue that although many techniques have been developed to detect the source of large packet and widespread packet flows but there is no technique to keep a track of individual packets. This technique generates audit trials for traffic within the network so the origin of a single IP packet can be traced back efficiently. They have developed a Source Path Isolation Engine (SPIE) which uses bloom filters and stores only packet digests instead of packet themselves. This also preserves confidentiality. They have made use of enhanced routers which maintain a cache of packet digests by making use of Data Generation Agent (DGA) which stores the digests in bit mapped form. Although it suggests that SPIE is able to identify the transformed IP packet but due to stateless nature of IP networks, many transformations are not invertible without additional memory overheads.

Bellovin et al. (2003) proposed a new Internet Control Message Protocol (ICMP) message which signals the attacked party of the attack being performed. These ICMP messages are randomly forwarded by the intermediate routers all the way till the destination or the victim site. When enough of such traceback messages are spread the traffic source of the forged packets can be determined. This is opposite to the traceroute command which provide the forward path and not the backward or traceback path. This traceback message is Hash Message Authentication Code (HMAC) authenticated and is carried in ICMP packet which must contain the link of either forward packet or the backward packet. This scheme is limited to the cases where the attack sources are less in number and effective rotation of the hash keys used is still an open challenge.

OPEN RESEARCH ISSUES AND CHALLENGES

There are many open research issues and challenges in the amalgamated area of economics and information security. These problems not only involve the application of economics and cyber security but also of other research domains like algorithm design, computer networks, customer psychology and management of resources.

Algorithm Mechanism

As the information security regulations are not standardized globally so designing algorithms which are cheat-proof is an open research area which the researchers are exploring strategy-based mechanisms (Nisan & Ronen, 1999) which ensure that the illegitimate behavior is avoided at the design level instead of rectifying after deployment.

Fair Allocation

Fair allocation of already scarce network resources is a key challenge in any payment structure. There is already a collection of various auction mechanisms like combinatorial, bundled (Feigenbaum et al., 2005) but the issue that arises in them is the exponential growth in the number of bits used for communication which causes complexity issues even for a small group.

Network Analysis

Conflict dynamics of any network is strongly influenced by its topology because the robustness properties of different topologies are different. The main aim of the attacker is often to disconnect the victim machine from the rest of the network. The concept of scale free networks has been discussed by Albert et al. (2000). They are very robust networks which mimic the real-world networks but on removal of nodes having higher order the connectivity of the network collapses.

Degree Distribution

On focusing why the networks with individual costs of link connectivity which outweigh the overall community benefit are created leads us to the open research issue of degree distribution. Although the attacks on the degree centrality of the internet have been rare but it plays an important role in its structure (2004) because the backbone ISP routers have lower degree as compared to the home routers.

Project Failures

The study of internet economics has helped the researchers in the field of computer systems management. In handling computer systems, the largest risk is of project failure which costs millions in large project undertakings. Although better tools are available to work with larger systems, but still the failure rate remains constant at 30% (Curtis et al., 1988).

Human Psychology

Designing any policy for charging the internet use is based on human psychology in many ways. First factor is the degree of difficulty with which the user will be affected by peers and forced by certain illegit authorities to behave maliciously. A group of people then behave inappropriately like calling up and chasing prospective credit card holders to get their personal details. Second is the usability and third is deception (Cranor & Garfinkel, 2005). The problem of camouflaging and phishing comes under this classification. The fundamentals of the attackers which motivate then to take part in attack are based on highly realistic rationale and theory of mind leading to self-interest.

CONCLUSION

Over the past years, the research area of internet economics has generated many useful works having an interdisciplinary approach. Long unknown things to the security professionals like incentives and market failure is now taken into consideration before designing any payment structure. The work being carried out in internet domain field has spread across various other domains like algorithmic design, security and warfare, interconnected networks and dependability economics of these complicated networks. Psychology has proved to be an important consideration while developing practical schemes for internet pricing. It gives a deeper understanding of fundamental user behavior which helps in making the scheme more usable and secure.

ACKNOWLDGMENT

This publication is an outcome of the R&D work undertaken under: i) project grant (SB/FTP/ETA-131/2014) from SERB, DST, Government of India; and ii) YFRF of the project Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India and being implemented by Digital India Corporation.

REFERENCES

Adat, V., Dahiya, A., & Gupta, B. B. (2018, January). Economic incentive based solution against distributed denial of service attacks for IoT customers. In *Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-5). IEEE. doi:10.1109/ICCE.2018.8326280

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. *nature, 406*(6794), 378.

Alomari, E., Manickam, S., Gupta, B., Karuppayah, S., & Alfaris, R. (2012). Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. *International Journal of Computers and Applications*, *49*(7), 24–32. doi:10.5120/7640-0724

Anderson, R. J. (1994). Why Cryptosystems Fail. *Communications of the ACM*, *37*(11), 32–40. doi:10.1145/188280.188291

Bailey, J. P. (1997). The economics of Internet interconnection agreements. *Inter Economics*, *35*, 155–168.

Belenky, A., & Ansari, N. (2003). IP traceback with deterministic packet marking. *IEEE Communications Letters*, *7*(4), 162–164. doi:10.1109/LCOMM.2003.811200

Bellovin, S. M., Leech, M., & Taylor, T. (2003). ICMP traceback messages.

Bichler, M. (2001). *The future of e-markets: multidimensional market mechanisms*. Cambridge University Press. doi:10.1017/CBO9780511492532

BoyleJ.DurhamD.HerzogS. (2000). COPS usage for RSVP.

Cao, Z., & Zegura, E. W. (1999, March). Utility max-min: An application-oriented bandwidth allocation scheme. In *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now* (Vol. 2, pp. 793-801). IEEE.

Chhabra, M., Gupta, B., & Almomani, A. (2013). A novel solution to handle DDOS attack in MANET. *Journal of Information Security*, *4*(3), 165–179. doi:10.4236/jis.2013.43019

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc.

Curtis, B., Krasner, H., & Iscoe, N. (1988). A field study of the software design process for large systems. *Communications of the ACM*, *31*(11), 1268–1287. doi:10.1145/50087.50089

Das, S. K., Jayaram, R., Kakani, N. K., & Sen, S. K. (2000). A call admission and control scheme for quality-of-service (QoS) provisioning in next generation wireless networks. *Wireless Networks*, *6*(1), 17–30. doi:10.1023/A:1019160708424

Dean, D., Franklin, M., & Stubblefield, A. (2002). An algebraic approach to IP traceback. *ACM Transactions on Information and System Security*, *5*(2), 119–137. doi:10.1145/505586.505588

Dellarocas, C. (2001, October). Analyzing the economic efficiency of eBay-like online reputation reporting mechanisms. In *Proceedings of the 3rd ACM Conference on Electronic Commerce* (pp. 171-179). ACM. doi:10.1145/501158.501177

Elwalid, A., Mitra, D., & Wentworth, R. H. (1995). A new approach for allocating buffers and bandwidth to heterogeneous, regulated traffic in an ATM node. *IEEE Journal on Selected Areas in Communications*, *13*(6), 1115–1127. doi:10.1109/49.400666

Feigenbaum, J., Papadimitriou, C., Sami, R., & Shenker, S. (2005). A BGP-based mechanism for lowest-cost routing. *Distributed Computing*, *18*(1), 61–72. doi:10.1007/s00446-005-0122-y

Geng, X., Huang, Y., & Whinston, A. B. (2002). Defending wireless infrastructure against the challenge of DDoS attacks. *Mobile Networks and Applications*, *7*(3), 213–223. doi:10.1023/A:1014526713037

Geng, X., & Whinston, A. B. (2000). Defeating distributed denial of service attacks. *IT Professional*, *2*(4), 36–42. doi:10.1109/6294.869381

Gupta, A., Stahl, D. O., & Whinston, A. B. (1995). A priority pricing approach to manage multi-service class networks in real-time. *The Journal of Electronic Publishing*, *1*(1&2).

Gupta, A., Stahl, D. O., & Whinston, A. B. (1996). An economic approach to networked computing with priority classes. *Journal of Organizational Computing and Electronic Commerce*, *6*(1), 71–95. doi:10.1080/10919399609540269

Gupta, A., Stahl, D. O., & Whinston, A. B. (1999). The economics of network management. *Communications of the ACM*, *42*(9), 57–63. doi:10.1145/315762.315772

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). Handbook of research on modern cryptographic solutions for computer and cyber security. Hershey, PA: IGI Global. doi:10.4018/978-1-5225-0105-3

Huang, Y., Geng, X., & Whinston, A. B. (2007). Defeating DDoS attacks by fixing the incentive chain. *ACM Transactions on Internet Technology*, *7*(1), 5, es. doi:10.1145/1189740.1189745

Kelly, F. (1997). Charging and rate control for elastic traffic. *European transactions on Telecommunications, 8*(1), 33-37.

Keshav, S., & Kesahv, S. (1997). *An engineering approach to computer networking: ATM networks, the Internet, and the telephone network* (Vol. 1). Reading: Addison-Wesley.

Lee, J. S., & Hoh, B. (2010, March). Sell your experiences: a market mechanism based incentive for participatory sensing. In *Proceedings of the 2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (pp. 60-68). IEEE. doi:10.1109/PERCOM.2010.5466993

Li, L., Alderson, D., Willinger, W., & Doyle, J. (2004, August). A first-principles approach to understanding the internet's router-level topology. *Computer Communication Review*, *34*(4), 3–14. doi:10.1145/1030194.1015470

Li, W., Yu, J., Cheng, X., Bie, R., & Zhao, F. (2016). An extensible and flexible truthful auction framework for heterogeneous spectrum markets. *IEEE Transactions on Cognitive Communications and Networking*, *2*(4), 427–441. doi:10.1109/TCCN.2016.2620973

Mei, A., & Stefa, J. (2012). Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals. *IEEE Transactions on Dependable and Secure Computing*, *9*(4), 569–582. doi:10.1109/TDSC.2012.37

Mousa, H., Mokhtar, S. B., Hasan, O., Younes, O., Hadhoud, M., & Brunie, L. (2015). Trust management and reputation systems in mobile participatory sensing applications: A survey. *Computer Networks*, *90*, 49–73. doi:10.1016/j.comnet.2015.07.011

Negi, P., Mishra, A., & Gupta, B. B. (2013). Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment. *International Journal of Computer Science Issues*, *10*(2 Part 1), 142.

Nisan, N., & Ronen, A. (1999). Algorithmic mechanism design extended abstract. In: STOC '99, pp. 129–140. doi:10.1145/301250.301287

Savage, S., Wetherall, D., Karlin, A., & Anderson, T. (2001). Network support for IP traceback. *IEEE/ACM Transactions on Networking*, *9*(3), 226–237. doi:10.1109/90.929847

Sloman, M. (1994). Policy driven management for distributed systems. *Journal of Network and Systems Management*, *2*(4), 333–360. doi:10.1007/BF02283186

Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Kent, S. T., & Strayer, W. T. (2001, August). Hash-based IP traceback. *Computer Communication Review*, *31*(4), 3–14. doi:10.1145/964723.383060

Song, D. X., & Perrig, A. (2001). Advanced and authenticated marking schemes for IP traceback. In *Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society* (Vol. 2, pp. 878-886). IEEE.

Varian, H. (2015). Keynote address to the Digital Rights Management Conference, Berlin, Germany.

Yavatkar, R., Pendarakis, D., & Guerin, R. (2000). *A Framework for Policy-based Admission Control RSVP.*

B. B. Gupta received a PhD degree from Indian Institute of Technology Roorkee, India in the area of information security. He has published more than 50 research papers in international journals and conferences of high repute. He has visited several countries to present his research work. His biography has published in the Marquis Who's Who in the World, 2012. At present, he is working as an Assistant Professor in the Department of Computer Engineering, National Institute of Technology Kurukshetra, India. His research interest includes information security, cyber security, cloud computing, web security, intrusion detection, computer networks and phishing.

Prachi Gulihar received a Masters's degree in Computer Engineering from National Institute of Technology-Kurukshetra, India. Earlier in 2016, she graduated from the First State Women University of North India, BPSMV in Computer Science Engineering. At present, she is working with Research Team of Cloud Vertical in Samvardhana Motherson Group of Companies as Software Engineer. She has published Book Chapters and Research Papers in the area of Financial Cryptography involving Bitcoin and Economic Incentive based Solutions for DDoS. She is ardent about Industrial IoT, JAVA applications and Cloud Services. Also, she is an environmentalist at heart and loves speaking French.