Using Game Theory to Classify Wireless Ad Hoc Network Attacks with Analysis on Countermeasures

[1*]Xiaojuan Liao, [2*]Dong Hao, [3]Kouichi Sakurai
[*1] *Department of Informatics, Kyushu University, liao@itslab.inf.kyushu-u.ac.jp*
[2] *Department of Informatics, Kyushu University, haodong@itslab.inf.kyushu-u.ac.jp*
[3] *Department of Informatics, Kyushu University, sakurai@csce.kyushu-u.ac.jp*

Abstract

Game theory has been receiving immense concern to deal with attacks in wireless ad hoc networks, which are widely employed in a large range of applications but vulnerable to various attacks. Previous works provided readers with comprehensive understanding of game theoretic solutions on cyber security problems. However, they neglect the relationship between attack characteristics and the corresponding game features. In this paper, we study the application of game theory on attacks in wireless ad hoc networks. Specifically, we present a classification which associates attack characteristics with types of game players and then examine the relationship between attack scenarios and types of corresponding game models. By illustrating the different players and game types in a variety of game theoretic approaches, we provide a comprehensive view on game based solutions to attacks in wireless ad hoc networks.

Keywords*: Attack Classification, Game Theoretic Analysis, Wireless Ad Hoc Network*

1. Introduction

1.1. Background

Wireless ad hoc network is suitable for a variety of applications such as the battlefield environment and emergency response. However, the security concerns remain an impediment to widespread adoption [1]. Generally, wireless ad hoc networks have some special characteristics that distinguish from other networks, in terms of self-organized entities, distributed operation, multi-hop routing, open medium, and limited energy, etc**.** Many routing protocols have been proposed for wireless ad hoc networks and improvements aim to optimize the original routing protocols, in terms of decreasing the route discovery latency [2] and increasing the packet delivery rate [6]. However, since packet delivery heavily relies on the cooperation of relay nodes and nodes are autonomous without any enforced centralized management, correctly running these well-designed routing protocols is challenged by a variety of attacks.

Conventional cryptography and intrusion detection systems provide the first line of defense in networks, nevertheless, standard cryptography may be of little use in presence of inside attacks, and traditional intrusion detection systems may fail in identifying variants of attacks. Recently, game theoretic approaches have attracted immense attention in fighting against wireless ad hoc network attacks. It provides rich mathematical tools for resolving multi-criteria optimization problems among multiple entities who behave strategically.

1.2. Related works

Previous researches have devoted tremendous effort on the security issues in wireless ad hoc networks great work on the classification of attacks and countermeasures. In the area of network attacks, Wu *et al.* [14] sorted attacks according to the existing network structure in mobile ad

∗ The first and second authors are supported by the governmental scholarship from China Scholarship Council.

This work was partly supported by Grants-in-Aid for Scientific Research (B) (23300027), Japan Society for the Promotion of Science (JSPS).

hoc networks and sensor networks. In the area of game theory, Manshaei *et al.* [10] showed the research status on game applications, and Saad [15] classified game theoretic approaches according to different game types, namely, the static or dynamic game with the complete or incomplete information. These works provide readers with comprehensive understanding of game theoretic solutions on cyber security problems. However, oddly enough, there is little effort devoted to investigating the association between attack scenarios and game theory. To date, which kind of attacks is suitable to be thwarted by game theory remains unanswered.

1.3. Our contribution

We study the application of game theory on attacks in wireless ad hoc networks. Specifically, we make the following contributions:

A classification is presented, grouping a variety of attacks into two categories, labeled with *palpable attack* and *subtle attack*. We find that players in game theoretic approaches vary regularly according to the two categories. This regularity can help construct game models against attacks.

A variety of game models are utilized by researchers in dealing with large number of attacks. We examine the relationship between attack scenarios and types of corresponding game theoretic approaches. Our work is to summarize some common features of these game models. We believe our work plays an instructive role in the game design to counter attacks.

2. Classification of attacks

We propose a new classification, which sorts prevalent attacks into *palpable attack* and *subtle attack*. Palpable attacks result in conspicuous impacts on network functions and the impacts are intolerable to users, while subtle attacks lead to invisible damages in vaguer way. Common attacks are labeled with either palpable attacks or subtle attack, shown as follows:

- *Palpable Attack*s: Jamming, Traffic Manipulating, Blackhole, Flooding.

In jamming (in physical layer) and traffic manipulating attacks (in medium access layer), attackers deliberately send signals to interrupt normal communications. In blackhole attacks, adversaries first attract traffic from normal nodes and then constantly discard all packets passing by them. In flooding attacks, adversaries send too many requests which overwhelm the target, so that disable the normal communications. Damages caused by these attacks are so conspicuous that normal nodes are aware of. Therefore, normal nodes can play games directly with attackers without any new players or extra mechanisms, though these designs can enhance the effectiveness.

- *Subtle Attacks*: Eavesdropping, Traffic Monitoring, Grayhole, Wormhole, Sybil Attack.

In eavesdropping (in physical layer) and traffic monitoring attacks (in medium access layer), attackers passively listen to communications and analyze the traffic without intercepting normal communications. In grayhole attacks, adversaries partially drop a selective set of packets passing through them. The partial packet loss confuses normal nodes on whether it is caused by intentionally malicious nodes or due to temporary traffic jamming. In wormhole, attackers collaborate to convince victims that two remote nodes are neighbors. In Sybil attacks, an adversary takes on multiple identities in the network. These attacks pave the way for further advanced attacks by confusing normal nodes, but never cause any conspicuous damages unless followed by further attacks. Because of the inconspicuousness of subtle attacks, normal nodes can hardly play games directly with attackers. According to our study, there are mainly two ways to suit game models in subtle attacks. Firstly, new players are introduced to play the role of helpers, who observe or withstand malicious behaviors actively. In addition, normal nodes can monitor the network flow to capture misbehavior with the help of complementing security mechanisms such as the reputation and voting systems. Both of the two methods rely on active observations. In addition to the aforementioned methods, both palpable and subtle attacks can be tackled by coalitional game played among cooperative wireless users.

Now we have identified the regularity of game players in game models against wireless ad hoc network attacks. The following sections analyze the types of game models against these attacks and find out deep relationship between attack scenarios and types of game models.

3. Palpable attacks

3.1. Jamming and traffic manipulating

- *Game Models: Zero-sum / Constant-sum Game, Coalitional Game.*

In jamming attacks, adversaries actively transmit signals concurrently when wireless nodes begin to do so, thus interrupting and interfering with the communication channels. Wireless users are aware of a jamming attack when their communications are disturbed by unexpected interruptions, thus normal nodes can play a game directly between jamming attackers.

In jamming scenarios, legitimate users and jammers have absolutely opposite objective profiles, in which legitimate users seek to maximize the ratio of the reliable information in transmission, while adversaries try to minimize the same quantity. The conflict of the interest is captured by the *constant-sum or zero-sum game* [9], in which the cost of a player is equal to the gain of the other. Although in existing literature, the effectiveness of the communications is measured in different ways, all the objective functions indicate the ratio of reliable information in communications. In addition, the sender and receiver can cooperate to eliminate jammers, playing the *coalitional game* [7].

The traffic manipulating attack is a kind of jamming attack in the medium access layer. Similar to jamming, the obvious evidences of attackers make normal nodes be able to play games with attackers, and the conflicting interest can be modeled as the *zero-sum game*/*constant-sum game* [11].

3.2. Blackhole

- *Game Model: Stochastic Game.*

Blackhole is one of the typical attacks which refer to intentional packet dropping. Two stages consist of a blackhole attack. In the first stage, a malicious node attracts traffic by advertising himself as having the freshest and shortest path to the destination. In the second stage, the attacker wreaks havoc by dropping all packets passing by him. The sender can be aware of the attacker existing in the route when he fails to receive any response (including link error messages) from the destination. Therefore, normal nodes can play games with attackers directly.

A blackhole attack occurs along with the packet delivery which usually repeats many times, and neither normal nodes nor attackers can know when the current packet delivery will end. Under this situation, players have more than one chance to adjust their strategies in these multiple stages. Moreover, the multiple stages are interdependent and transferable in line with the previous stage and the actions chosen by players, thus a *stochastic game* forms. Shila *et al.* [3] proposed a stochastic game to tackle the blackhole, played between a source node and its downstream node. There are four states in the game. Each of them is defined as (m, n), where m is the state of the sender buffer and n is the state of the drop buffer. (m,n) reflects the buffer states of both the sender and the relay node. A source node has two strategies, namely, to send the packet directly to the destination or to send the packet through a relay node. Passing packets to a relay node can save energy but implies greater threat as critical relay nodes are likely to be malicious. The relay node also has two strategies, i.e., transmit the packet or drop the packet. For an attacker, he always tries to discard as many packets as possible, but once he is discovered, the source node would choose another route and the attacker cannot benefit any more. In each stage, both the source node and relay node choose their actions according to the outcome of the last stage and then make the game move to a new stage. Shila *et al.* concluded that when the dropping probability of the attacker increases, the source would switch to a secure but high cost path with higher probability. It is worth noting that although Shila *et al.* aim at defeating grayhole attack, we will explain in the next section that the ideal grayhole attack, which does not contain the network link errors, is the same as the blackhole attack.

3.3. Flooding

- *Game Models: Symmetric Game, Repeated Game.*

A flooding attacker sends an overwhelming number of requests to the target, so as to disable the target's service for legitimate nodes. Legitimate nodes can actively conquer flooding attacks via either restricting the number of requests initiated by a single source, or limiting the number of requests rushing to one target. In the first case, legitimate users can cooperate to constrain the total number of packets flowing through the network. An example is the symmetric forward dilemma game [17]. Although the original intention was to reduce the number of overhead packets rather than handling the flooding attack, it still can partially work. Every node decides whether to deliver the incoming packet. Packet delivery by any node can benefit all the neighbors. The symmetry of nodes causes the gain and cost of all the nodes are equal despite of the identities of players. This property is modeled in a *symmetric game*, where the payoffs depend only on the employed strategies rather than the identities of players. However, this method may hinder normal communications when the percentage of packets generated by one attacker overwhelms that of legitimate ones. One preferable way is to restrict the number of requests rushing to the same target. This method has an assumption that each node, including attackers, has the resource limitation. Fallah *et al.* [18] proposed a game based on such puzzles, played between a service provider and a requestor. A service provider sends a puzzle to his service requestor and asks him to solve. If the counterpart solves the puzzle correctly, then he would be served; otherwise he would not. The difficulty level of puzzles is critical. Difficult puzzles mean heavy burdens to legitimate users, while over-simple ones cannot prevent adversaries from attacking. As the attacker sends a large number of requests to the defender many times, and the action profiles are the same in the corresponding strategic-form games, the overall game between the defender and the attacker is a *repeated game*. The service provider adjusts the level of the puzzles, while a flooding attacker gains from consuming defender's energy, but has to waste energy on solving puzzles.

3.4. Summary

This section exemplified game theoretic approaches against palpable attacks in wireless ad hoc networks. Our investigation is shown in Table 1, which lists the game players and game models, as well as the exact properties of the corresponding game models. It is worth mentioning that these attacks can be tackled by many types of game models other than the listed ones. Our aim is to capture the significant properties of game models, which are suitable to be employed in dealing with attacks.

Table 1. Game players and models against palpable attacks

Attack Name	Game Player	Game Model	Property of the Game Model
Jamming / Traffic manipulating	Normal node and attacker	Zero-sum game Constant-sum game [9, 11]	Conflicting goals: normal nodes seek to maximize the ratio of the reliable information in transmission, while adversaries try to minimize the same capacity.
	Normal nodes	Coalitional game [7]	Common goals: Players cooperate for defeating jammers
Blackhole	Source node and potential attacker	Stochastic game [3]	Transferable multiple stages: In each stage, both the source node and relay node choose their actions according to the outcome of the last stage and then make the game move to a new stage.
Flooding	Normal node and attacker	Symmetric game [17]	Equal status of players: Packet delivery by any node can benefit all the neighbors, i.e., the gain and cost of all the nodes are equal despite of the identities of players.
		Repeated game [18]	Identical multiple stages: An attacker sends many requests to the defender in different stages, and the action profiles are the same in the corresponding strategic-form games.

4. Subtle attacks

4.1. Eavesdropping and traffic monitoring

- *Game Models: Dynamic Game, Coalitional Game.*

Eavesdropping and traffic monitoring belong to the same kind of attacks, which occurs in the physical layer and medium access layer, respectively. Attackers passively monitor the network and analyze the captured information that leaks from a communication channel without sending any interference signals actively.

Different from jamming, eavesdropping and traffic monitoring attacks are difficult to be perceived by victims since they do not cause any obvious impacts that normal nodes can identify. As a result, it is difficult to design a game directly played between normal nodes and attackers. Existing game solutions either introduce new players or define coalitional games between legitimate users. In the first case, Han *et al.* [12] introduced a friendly jammer who takes the responsibility of interrupting eavesdroppers at some power level. Another player, namely the legitimate node, adjusts the payment given to the employed jammer, thus in turn affects the power level devoted by the jammer to intercepting eavesdroppers. The property of sequential actions between legitimate users and friendly jammers can be captured by a *dynamic game*. As a typical example of the dynamic game, Stackelberg model is utilized, in which the legitimate user plays as a leader and the friendly jammer acts as a follower. In the latter case, Saad *et al.* [8] proposed a *coalitional game*, in which wireless users autonomously cooperate to defeat eavesdroppers. All users seek a tradeoff between the secrecy capacity lost in the eavesdropping attack and the equivalent capacity lost in the information exchange among users.

4.2. Grayhole

- *Game Models: Zero-sum Game, Dynamic Game.*

Both grayhole and blackhole attacks refer to intentional packet dropping. The main difference is that the blackhole attacker drops all the packets he receives while the grayhole attacker only drops a certain fraction of packets. Therefore, normal nodes may be not aware of this advanced selective dropping attack as they may not know whether the packet loss is caused by intentional attackers or temporarily jammed network. Conventionally, effect of network status was ignored, thus any percentage of packet loss is viewed as the existence of attackers. Under this assumption, game methods against grayhole and blackhole have no difference. However, the elimination of traffic status is unrealistic and fails to characterize grayhole attacks. A more reasonable way is to take links error into consideration. In this case, even benign nodes may discard packets due to the network congestions, and the grayhole attacker seems scot-free if normal nodes do not pay more attention to conducting detection. To fight against the complicated grayhole attacks in presence of link errors, game models have to introduce IDS node and employ additional security mechanisms. In Reddy et al. [13], network is divided into several clusters. In each cluster, there is an IDS node responsible to detect attackers. IDS nodes aim to protect the network at the cost of reasonable energy while attackers intend to destroy the network by consuming IDS as more energy as possible. The conflicting goal of the two players is modeled in a *zero-sum game*. Another game is a *dynamic game* played between a normal node and an attacker [4]. The game is composed of sequential stages: firstly, the source requests some players to be on a certain route to the destination and decides whether to use this route to send a packet; then each relay node decides whether to forward this packet once it has received it. This model is based on the imperfect detection and security mechanisms, incorporated with the access control, authentication, data integrity etc.

4.3. Wormhole

- *Game Model: Stochastic Game.*

Wormhole occurs in the routing layer where one attacker captures packets from one location and tunnels them to the colluding node. The tunnel between the two colluding attackers is called wormhole.. A wormhole attack creates an illusion that two remote nodes are neighbors. In fact, it does not cause any actual damages to victims unless followed by further palpable attacks such as packet

dropping. To detect a pure wormhole attack, active observations and complementing mechanisms are necessary, but they do not always work due to the attack methods. A wormhole tunnel can be established via two ways, i.e. out-of-band channel and in-band channel. Particularly, out-of-band attack is achieved by separate communication channel, exclusively utilized by attackers and cannot be accessed by normal users. Thus, the interaction between defenders and attackers can be hardly defined, which leads to rare use of game theory. By contrast, in-band wormhole attack is achieved by packet encapsulation. Although intermediate nodes may have no access to the contents of packets, they can detect malicious behaviors by observing packet streaming passing by them. To conquer the in-band wormhole, Baras *et al.* [16] proposed a *stochastic game* played between IDS nodes and attackers. The IDS node takes the responsibility to detect attackers actively, trying to minimize the number of required observation samples to restrict the ratio of false detections, while attackers tune the length of tunnel according to the utilities of the last stage. Indeed, a long tunnel enhances the attack, but it increases the risk of being detected at the same time.

4.4. Sybil attack

- *Game Models: Signaling Game, Dynamic Game, Repeated Game.*

The Sybil attack means one malicious node feigns multiple identities in a network, by either creating a new identity or stealing the identity of an existing node. Sybil attack poses a large number of potential threats to reputation systems, routing protocol, and affect fair resource allocation as well as the malicious detection.

In general, a Sybil attack can be utilized as the preliminary step for further attacks. When a Sybil node successfully falsifies identities, these Sybil identities can strategically choose to either misbehave or pretend to be legitimate for advanced attacks. The uncertainty in whether to mount attacks leads to difficulty in detecting Sybil nodes unless they launch further attacks or legitimate nodes take active actions to detect attackers. Game models are built to allure Sybil nodes to confess, providing that the confessing reward paid for Sybils exceeds the amount that Sybils earn from the fake identities. Margolin *et al.* [19] proposed a *signaling game*, played between a detective and other nodes. The detective launches a game to find whether there are Sybils in the network and other nodes take actions according to their types, e.g., non-Sybil, low-profit-Sybil, or high-profit Sybil. These types are given by nature and are not known by the detective. Players choose actions according to their types, and the detective can infer the types of his opponents by observing the actions of them. Margolin *et al.*proved that only Sybil nodes play the game, and only low-profit Sybil nodes are willing to play the game at the beginning stage. Later, Pal et al. [20] put forward a feedback mechanism-based *dynamic game*, named Sybil Detection Game (SDG). When a detective initiates a game, other players choose whether to join or quit the game, then the detective checks if negotiation is required to determine the reward amount. After that, players choose their strategies on whether to tell honestly about their identities and whether to give correct feedbacks about others. This game successfully encourages all participants to reveal Sybil identities. However, the aforementioned game models provide a chance for Sybil nodes to gain more than non-Sybils, thus the phenomenon of Sybil nodes cannot be eradicated. More recently, a reputation systems based *repeated game* was proposed [5]. Similar to the puzzle-based game against flooding, this game is modeled between a service provider and a requestor. The author mapped the actions of Sybil attackers into service requests. When a player makes a request, he has the opportunity to deploy sufficient number of his Sybil identities to launch an effective attack. For a service provider, he can strategically choose to reply the request or not. The process of challenge and reply usually repeat many stages and in each stage, the action profiles are the same, thus the overall game is a repeated game. It proved that the Sybil attack can be thwarted if the attacker’s profit from deceiving a single node is less than the minimum cost required for an effective attack.

4.5. Summary

This section investigated various types of game models against subtle attacks, shown in Table 2. Also, in addition to the mentioned game models, there are many other types of game models which can be utilized to tackle attacks as long as we could find the deep relationship between the properties of attacks and game models.

Table 2. Game players and models against subtle attacks

Attack Name	Game Player	Game Model	Property of the Game Model
Eavesdropping / Traffic monitoring	Normal node and additional helper	Dynamic game [12]	Sequential actions: A friendly jammer adjusts the energy level to help intercept attackers according to the payment given by the legitimate node.
	Normal nodes	Coalitional game [8]	Common goals: Players autonomously cooperate to defeat eavesdroppers.
Grayhole	Detective node and attacker	Zero-sum game [13]	Conflicting goals: IDS nodes protect the network at a reasonable energy cost while attackers intend to destroy the network by consuming IDS as more energy as possible.
	Detective node and potential attacker	Dynamic game [4]	Sequential actions: firstly, the source takes actions on whether to send a packet to a relay node; then the relay node decides whether to forward this packet.
Wormhole	Detective node and potential attacker	Stochastic game [16]	Transferable multiple stages: In each stage, both players choose actions according to the outcome of the last stage and then make the game move to a new stage.
Sybil attack	Detective node and potential attacker	Signaling game [19]	Unilaterally unknown players: Players choose actions according to their types, which are given by nature and unknown by the detective. The detective can infer the types of his opponents by observing the actions of them.
		Dynamic game [20]	Sequential actions: the detective checks if negotiation is required, then potential attackers choose strategies according to the payment given by the detective.
	Service provider and requestor	Repeated game [5]	Identical multiple stages: In multiple-stage interactions between the service requestor and provider, the action profiles keep the same.

5. Conclusion

This paper has presented a classification which associates the characteristics of attacks with types of game players, and studied the relationship between attack characteristics and types of corresponding game models. By investigating the different players and game types in a variety of game theoretic approaches, we provided a comprehensive view on game based solutions to attacks in wireless ad hoc networks. We believe our classification on attacks and analysis on the game models can significantly help to design effective game theoretic approaches.

6. References

[1] F. Anjum, P. Mouhtaris, “Security of Wireless Ad Hoc Networks”, Wiley, USA, 2007.
[2] M. H. Mamoun, “A New Routing Scheme for MANET”, Journal of AICIT, Advances in Information Sciences and Service Sciences, vol. 2, no. 1, pp. 6-15, 2010.
[3] D. M. Shila, T. Anjali, “A Game Theoretic Approach to Gray Hole Attacks in Wireless Mesh Networks”, In Proceedings of Military Communications Conference, pp. 1-7, 2008.

[4] W. Yu, Z. Ji, K. J. Ray Liu, "Securing Cooperative Ad-Hoc Networks under Noise and Imperfect Monitoring: Strategies and Game Theoretic Analysis", IEEE Transactions on Information Forensics and Security, vol. 2, no. 2, pp. 240-253, 2007.
[5] M. S. Fallah, M. Mouzarani, "A Game-based Sybil-Resistant Strategy for Reputation Systems in Self-Organizing MANETs", Computer Journal, vol. 54, no. 4, pp. 537-548, 2011.
[6] M. H. Mamoun, "A New Proactive Routing Protocol for MANET", Journal of AICIT, Advances in Information Sciences and Service Sciences, vol. 3, no. 2, pp. 132-140, 2011.
[7] S. Mathu, L. Sankar, N. B. Mandayam, "Coalitions in Cooperative Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 26, no. 7, pp. 1104-1115, 2008.
[8] W. Saad, Z. Han, T. Basar, M. Debbah, A. Hjrungnes, "Physical Layer Security: Coalitional Games for Distributed Cooperation", In Proceeding of 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless, pp. 1-8, 2009.
[9] E. Altman, K. Avrachenkov, A. Garnaev, "Jamming in Wireless Networks under Uncertainty", Mobile Networks and Applications, vol. 16, no. 2, pp. 246-254, 2011.
[10] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. P. Hubaux, "Game Theory Meets Network Security and Privacy", EPFL Technical Report, 2010.
[11] Y. E. Sagduyu, R. Berry, A. Ephremides, "MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types", In Proceedings of 20th International Conference on Game Theory for Networks, pp. 130-139, 2009.
[12] Z. Han, N. Marina, M. Debbah, A. Hjorungnes, "Physical Layer Security Game: Interaction between Source, Eavesdropper, and Friendly Jammer", EURASIP Journal on Wireless Communications and Networking - Special issue on wireless physical layer security, vol. 2009, no. 11, pp. 1-10, 2010.
[13] T. B. Reddy, S. Srivathsan, "Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks", In Proceedings of 17th Mediterranean Conference on Control and Automation, pp. 458-463, 2008.
[14] Yang Xiao, Xuemin Sherman Shen and Ding-Zhu Du, "Wireless Network Security", Springer, Germany, 2007.
[15] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, T. Basar, "Coalitional Game Theory for Communication Networks: a tutorial", IEEE Signal Processing Magazine, vol. 26, no. 5, pp. 77-97, 2009.
[16] J. S. Baras, S. Radosavac, G. Theodorakopoulos, D. Sterne, P. Budulas, R. Gopaul, "Intrusion Detection System Resiliency to Byzantine Attacks: the Case Study of Wormholes in OLSR", In Proceedings of IEEE Military Communications Conference, pp. 1-7, 2007.
[17] N. Mhammad, T. Kemal, "Game Theoretic Approach in Routing Protocol for Wireless Ad Hoc Networks", Ad Hoc Networks, vol. 7, no. 3, pp. 569-578, 2009.
[18] M. S. Fallah, "A Puzzle-based Defense Strategy against Flooding Attacks Using Game Theory", IEEE Transactions on Dependable and Secure Computing, vol.7, no. 1, pp. 5-19, 2010.
[19] N. Boris Margolin , Brian N. Levine, "Informant: Detecting Sybils Using Incentives," Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security, pp. 12-16, 2007.
[20] A. K. Pal, D. Nath, S. Chakreborty, "A Discriminatory Rewarding Mechanism for Sybil Detection with Applications to Tor", Word Academy of Science, Engineering and Technology, vol. 63, no. 6, pp. 29-36, 2010.