RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Mitigating Denial-of-Service Attacks in MANET by Incentive-Based Packet Filtering

[1]Shaik Noor Mohammad & [2]Dr. R. Mohan Kumar

[1]*Research Scholar, Sri Satya Sai University, Sehore M.P. (India)*
[2]*Research Guide, Sri Satya Sai University, Sehore M.P. (India)*

ARTICLE DETAILS

Article History
Published Online: 15 May 2019

Keywords
MANET, Security, AODV, Routing Attacks, DoS.

ABSTRACT

Safeguarding against refusal of-administration (DoS) in a portable specially appointed system (MANET) is testing on the grounds that the system topology is dynamic and hubs are egotistical. In this paper, we propose a DoS relief strategy that utilizes advanced marks to check genuine bundles, and drop parcels that don't pass the confirmation. Since hubs are narrow minded, they may not play out the check with the goal that they can abstain from paying the overhead. An awful bundle that escapes check along the entire system way will convey a punishment to all its forwarders. A system amusement can be figured in which hubs along a system way, in improving their very own advantages, are urged to act by and large to sift through terrible parcels. Investigative outcomes demonstrate that Nash harmony can be accomplished for players in the proposed amusement, in which noteworthy advantages can be given to forwarders to such an extent that a large number of the terrible parcels will be disposed of by check.

1. Introduction

The conditions between unique, commonly untrusted neighbors in a versatile specially appointed system (MANET) make significant security worries in such systems. Among the assaults archived in the writing, disavowal of-administration (DoS) assaults are especially harming since both correspondence transmission capacity and hub assets are rare in MANETs. Notwithstanding their capacity to bring down a system rapidly, DoS assaults coordinated at transfer speed and end hub assets are anything but difficult to dispatch; e.g., by basically infusing pointless traffic into the system. DoS alleviation methods intended for wireline systems won't function admirably in an impromptu domain where the courses and the arrangement of forwarders on a directing way are very powerful and are narrow minded. Secure directing conventions intended for impromptu systems [3] fabricate secure courses to help endto-end correspondence. In the event that connect layer security is connected [4], these conventions can relieve DoS assaults. Ill-conceived parcels will be found as outside aggressors don't have the foggiest idea about the keys shared between the bounces. Be that as it may, an inside assailant, i.e., an aggressor who is an individual from the start to finish way, can at present dispatch an assault. Without utilizing marks, it is hard to recognize the assailant regardless of whether the aggressor is known to be an insider. What's more, in systems where parcel conveyance is course based, these protected directing conventions can't be connected in light of the fact that the way can change from bundle to parcel. Spurring hubs to serve each other is another basic issue in MANETs. In particular, as correspondence endpoints depend on middle of the road hubs to advance their traffic, impetuses for the forwarders must be given. Conventional motivating force frameworks have utilized pieces [2] and notoriety credits [1] to urge hubs to work as forwarders. The motivating force issue turns out to be significantly increasingly pertinent in the security setting, when safety efforts may require certain hubs to exhaust more assets to all the more likely shield different hubs. The motivating force issue as it identifies with the security issue has been less tended to by the exploration network. In this work, we propose a DoS relieving system for MANETs that mutually thinks about the security and motivating force issues. The method is intended to work in a parcel exchanging system condition.

The thought depends on an aggressor's objective to keep away from identification and being recognized. Thus, we secure real parcels by expecting them to be marked by their individual senders. A forwarder checks a parcel's sender signature when the bundle is gotten. In the event that the confirmation comes up short, the bundle is dropped. Else, it is sent. We accept that organize hubs are childish however judicious. Motivating force for a hub to advance parcels is given by a reward the hub will get after the bundles are effectively conveyed to their last goals. A forwarder may likewise advance a bundle without check, since the activity conveys an expense. To inspire a forwarder to confirm, a punishment is evaluated for a "sluggish" hub each time it advances an aggressor bundle that at long last achieves the goal. We will explore the properties of the subsequent amusement, as forwarders autonomously endeavor to play a best sending/confirmation methodology that will amplify their own settlements, while the system is liable to given contributions of assaulting and real traffic. We utilize diversion hypothesis to examine how an arrangement of forwarders can be spurred to advance great parcels while sifting through awful bundles helpfully by confirmation. We will propose arrangements that address mutually the security and motivating force issues. We will talk about how commonsense cost capacities can be appointed for sending, sending, getting, and confirming.

2. Review of literature

Lu Han et al., depicts that the remote impromptu systems were first unfurled in 1990s. Portable specially appointed systems have been broadly inquired about for a long time. Versatile specially appointed systems are gathering of at least

two gadgets furnished with remote correspondences and systems administration capacity. Remote specially appointed Networks don't have a portal rather every hub can go about as the door. Albeit, bunches of research is done in this field, however the inquiry is frequently raised, regardless of whether the design of versatile impromptu systems is a key imperfect engineering.

Antonio Challita et al., portray various kinds of DDoS assaults, present ongoing DDoS safeguard techniques as distributed in specialized reports and propose a novel way to deal with counter DDoS. In view of basic barrier standards and considering the various kinds of DDoS assaults, this overview safeguard techniques and order them as per a few criteria. This work proposes an easy to-incorporate DDoS injured individual based barrier technique, Packet channeling, which goes for alleviating an assault's impact on the person in question. In this methodology, substantial traffic is piped before being passed to its goal hub, subsequently forestalling clog at the hubs get to connection and keeping the hub on-line. This technique is easy to coordinate, requires no joint effort between hubs, presents no overhead, and includes slight postpones just if there should arise an occurrence of overwhelming system loads. The bundle piping approach guarantees to be a reasonable methods for adapting to DDoS traffic, with simple mix at negligible expense in Framework for Statistical Filtering against DDoS Attacks in MANETs.

Hwee-Xian Tan and Winston K. G. Seah portrays that a DDoS (Distributed DenialOf-Service) assault is a dispersed, huge scale endeavor by noxious clients to flood the injured individual system with a tremendous number of bundles. This depletes the injured individual system of assets, for example, data transfer capacity, registering power, and so forth. The unfortunate casualty is unfit to give administrations to its authentic customers and system execution is enormously weakened. There are numerous techniques in the writing which intend to lighten this issue, for example, jump tally separating, rate-restricting and factual sifting. Notwithstanding, the vast majority of these arrangements are intended for the wired Internet, and there is little research endeavors on instruments against DDoS assaults in remote systems, for example, MANETs. This gives data about the helplessness of MANETs to DDoS assaults and give a diagram of measurable sifting, which is ordinarily utilized as a security system against DDoS assaults in wired systems and after that propose a structure for factual separating in MANETs to battle DDoS assaults. This likewise mimics some DDoS assaults in MANETs with no sifting systems to investigate and comprehend the impacts of such assaults on the exhibition of the system.

XianjunGeng et al., depicts that the infamous, devastating assault on online business top organizations in February 2000 and the common proof of dynamic system checking an indication of aggressors searching for system shortcomings everywhere throughout the Internet are harbingers of future Distributed Denial of Service (DDoS) assaults. They connote the proceeded with spread of the malevolent daemon programs that are probably going to prompt rehashed DDoS assaults within a reasonable time-frame. This gives data about system shortcomings that DDoS assaults abuse the innovative pointlessness of tending to the issue exclusively at the neighborhood level, potential worldwide arrangements, and why worldwide arrangements require a monetary motivation structure.

Qiming Li et al., depicts that Distributed Denial of Service (DDoS) assaults represent a genuine danger to support accessibility of the injured individual system by seriously debasing its exhibition. There has been huge enthusiasm for the utilization of measurable based separating to shield against and relieve the impact of DDoS assaults. Under this methodology, parcel measurements are checked to order ordinary and irregular conduct. Enduring an onslaught, bundles that are named unusual are dropped by the channel that watches the unfortunate casualty arrange. This gives the viability of DDoS assaults on such measurable based sifting in a general setting where the assailants are "keen". We first give an ideal arrangement for the channel when the factual practices of both the aggressors and the channel are static. Next, this considers situations where both the assailant and the channel can progressively change their conduct, potentially relying upon the apparent conduct of the other party. This sees while a versatile channel can viably protect against a static aggressor, the channel can perform much more regrettable if the assailant is more powerful than seen.

Kamanshis Biswas et al., referenced that Mobile Ad Hoc Network was an accumulation of imparting gadgets or hubs that desire to convey with no fixed framework. The hubs in MANET themselves are in charge of powerfully discovering different hubs in the system to convey. In spite of the fact that an impromptu system is utilized for business utilizes because of their specific one of a kind attributes, however the fundamental test is the weakness to security assaults. Various difficulties like unique system topology, stringent asset limitations, shared remote medium, open distributed net-work engineering, and so forth., are presented in MANET. As MANET is broadly spread for the property of its Capability in shaping brief system with no fixed foundation or concentrated topology, security challenges have turned into a main worry to give secure correspondence.

AndrimPiskozub et al., gives main sorts of DoS assaults, which flood injured individual's correspondence channel band-width, is done their investigation and are offered techniques for insurance from these assaults. The DDoS assaults are extensively more successful than their DoS partners since they permit performing such assaults at the same time from a few destinations that make this assault increasingly proficient and muddle hunts of an assailant. The aggressor utilizes the customer program, which, thusly, interfaces with the handler program. The handler sends directions to the operators, which perform real DoS assaults against a demonstrated systemvictim. This likewise depicts different countermeasures that ought to be taken to keep the system from DDoS assault.

XianjunGeng et al., depict that the famous, devastating assault on web based business' top organizations in February 2000 and the common proof of dynamic system filtering, an indication of assailants searching for system shortcomings

everywhere throughout the Internet, are harbingers of future Distributed Denial of Service (DDoS) assaults. They connote the proceeded with spread of the abhorrent daemon programs that are probably going to prompt rehashed DDoS assaults within a reasonable time-frame. This gives data about the shortcomings in the system that DDoS assaults misuse the mechanical uselessness of tending to the issue exclusively at the neighborhood level. Vicky Laurens et al., portray that because of money related misfortunes brought about by Distributed Denial of Service (DDoS) assaults; most resistance systems have been conveyed at the system where the objective server is found. This trusts this worldview should change so as to handle the DDoS danger in its premise: ruin operator machine's interest in DDoS assaults. This comprises of building up a specialist to screen the parcel traffic rate (active bundles/approaching parcels). The arrangement depends on describing TCP associations; ordinary TCP associations can be portrayed by the proportion of the sent parcels to the got bundles from a given goal. The outcome demonstrates that the traffic proportion esteems for the most part give bigger qualities toward the start of the run when there are insufficient parcels to settle on a choice that whether the traffic is real. A low an incentive for limit takes into account quicker discovery of assault, yet additionally expands the false-positives.

Stephen M. Specht portrays that Distributed Denial of Service (DDoS) assaults has turned into an enormous issue for the frameworks associated with the Internet. DDoS aggressors assume responsibility for optional unfortunate casualty frameworks and use them to dispatch a planned enormous scale assault against essential injured individual frameworks. Because of crisp counter estimates that are created to forestall or alleviate DDoS assaults, aggressors are always creating spic and span strategies to undermine these unused countermeasures. This likewise gives us data about DDoS assault models and the scientific classifications to describe the DDoS assaults, the product assaulting instruments utilized, and the potential countermeasures those are accessible. The scientific categorization demonstrates the similitudes and examples in various DDoS assaults, including new subordinate assaults. It is basic, that as the Internet and Internet utilization extend, increasingly exhaustive arrangements and countermeasures to DDoS assaults be created, checked, and executed all the more viably and correctly. DDoS assaults make an organized framework or administration inaccessible to authentic clients. These assaults are an inconvenience at any rate, or can be genuinely harming if a basic framework is the essential injured individual. Loss of The system assets causes financial misfortune, work postponements, and loss of correspondence between system clients. Arrangements must be created to anticipate these DDoS assaults.

3. Game Theoretic DoS Mitigation In MANET

Mitigating DoS in MANET

We necessitate that genuine sources carefully sign their bundles. Other than the system level steering data and the application level information payload, every bundle will likewise convey a marked MAC (Message Authentication Code), including an endorsement for the originator's open key. The marked MAC with the authentication is utilized to check that the parcel is from the asserted real source. In the event that the MAC conveyed in the parcel does not coordinate the MAC a forwarder creates from the got bundle, the parcel is named an awful parcel and consequently dropped. The mark based safeguard is inclined to the replay assault. An assailant can replay a real parcel countless to create a high heap of pointless traffic. These parcels will pass the check step. To manage the replay assault, a parcel ought to be stepped with its age time. What's more, every parcel has a given lifetime. A parcel whose life time has lapsed will be dropped. To keep a pernicious hub from sending a genuine bundle to various next jumps amid the parcel's lifetime, a neighbor observing system can be utilized. In neighbor checking, a hub peruses the total header, including both the MAC and system level headers, of each bundle regardless of whether the hub isn't the parcel's next bounce. The hub stores the header read until the relating parcel's lifetime terminates. After hearing a parcel whose lifetime has not terminated, the hub will contrast the header read and the headers at present in the hub's nearby store. By doing this, the hub can recognize a replayed parcel and drop it before further harm to the system occurs. Since just the parcel header, yet not the entire bundle, must be perused, the expense of observing will be kept low. In the event that the parcel lifetime isn't excessively long, which is regularly the situation in impromptu systems, a hub won't have to store such a large number of bundle headers, which lessens the capacity cost. Note that the checking method won't be successful in a wireline organize if aggressors select various courses for sending distinctive replayed bundles, since one forwarder will at that point be unfit to screen parcels bound for another forwarder. Fig. 1 demonstrates the proposed parcel group. In the figure, the past jump is the hub sending the parcel, and the following bounce is the hub assigned as the recipient of the sent bundle.

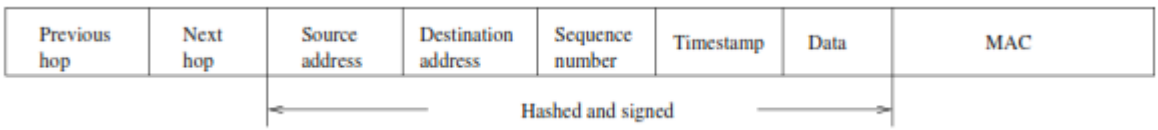

Figure 1: packet format.

On the off chance that each forwarder checks parcels before sending them, any assault traffic will be found and dropped to restrain its harm to the system. Specifically, end servers are relied upon not to get any assault bundle. System transmission capacity will likewise be to a great extent secured. Be that as it may, checking each bundle at each forwarder causes pointlessly high loads at the forwarders, particularly when a huge portion of the parcels is real.

To diminish the expenses of confirmation, without seriously trading off its viability, a forwarder may choose to probabilistically check a bundle. Since hubs are childish, we have to boost them to confirm with adequately high probabilities.

Incentives and game rationality

We apply a reward framework where hubs are given acknowledge for going about as forwarders. In particular, a forwarder is credited for sending a parcel if the bundle effectively lands at the goal. We accept the presence of a bookkeeping framework, like a "national bank", for safely monitoring the prizes, and anticipating tricking in asserting false rewards. In our DoS alleviation approach, the marked MAC of each sent parcel is put away at the forwarder. The put away MACs can be introduced to the bookkeeping framework as proof for gathering rewards. In the DoS flexible sending diversion, a hub's result is the reward for sending less the sending costs. The costs represent all used assets in the sending, for example, the vitality devoured for bundle get and transmission, and for playing out any required cryptographic activity. In the DoS resistance, forwarders check the MACs of got bundles. An egotistical forwarder may attempt to expand its result by not confirming, however depend on another forwarder on the bundle's course to check and achieve the activity of sifting through any assault parcel. Unmistakably, on the off chance that each forwarder reasons similarly and maintains a strategic distance from all check, at that point all assault bundles will be permitted to achieve their goals. To stay away from the degeneration of the DoS resistance into a framework in which no confirmation is performed by any means, a forwarder is rebuffed for sending an awful parcel that effectively makes it to the goal. Subsequently, if a forwarder presents the MAC of an awful bundle in asserting its reward, a punishment rather than a reward will be given. The punishment subtracts from the hub's all out credit for sending other great parcels. We plan the DoS strong bundle sending framework as a multiplayer amusement between forwarder hubs in a MANET. Forwarder hubs partake in a similar diversion on the off chance that they are on a similar course between a sender and collector. Since courses in a MANET can be exceedingly powerful, the arrangement of hubs playing against one another can change regularly. As talked about, a player's result in the amusement is its reward for sending the great parcels, less its punishment for sending the terrible bundles and its expenses of sending and confirmation. A player's methodology is its likelihood of checking a got parcel. The player's system might be versatile with the goal that the likelihood of check may change after some time.

4. Security goals for MANET

A definitive objective of the security answers for MANET is to give a structure covering [23] accessibility, secretly, respectability, and validation to safeguard the administrations to the portable client. A short clarification about these terms:- A. Accessibility Services of system ought to be accessible to validated clients. There ought to be sure component for assurance against such sort of assaults, which makes the system assets to inaccessible to approved clients like in the event of DOS (Denial of administration assault) assault, the accessibility of system and its assets would end up inaccessible to verified client . B. Classification Protection of data which is trading through a MANET ought to be ensured against any exposure assault like listening in unapproved perusing of message and traffic investigation done by an assailant hub to discover which sorts of correspondence is going on, as in the event of war regions it ends up basic to secure and verify such sort of correspondence. In MANET it is extremely hard to accomplish the classification as a result of middle of the road hubs directing, which can without much of a stretch listen the data which is being steered through them. C. Uprightness The data which is transmitted ought to be ensured against any change. Insurance against message change ought to be there. D. Confirmation The assets of system ought to be gotten to by the validated hubs. A portion of the verification strategies are:-

- Digital Signature: The sender hub signs the message carefully which will later confirm by the recipient hub carefully.
- Non denial: Ensures that sending and accepting gatherings can never deny each sending and getting of message.

5. Denial of service

Global Organization for Standardization (ISO) has given the accompanying definition for refusal of administration (DoS) in the standard ISO 7498-2:1989. Disavowal of administration: —The counteractive action of approved access to assets or the postponing of time-basic operations.‖ Open system engineering and shared transmission media make it conceivable to join a system without a physical association. It [18]

- Attempts to —flood‖ a system, in this way anticipating genuine system traffic
- Attempts to upset associations between two machines, accordingly anticipating access to an administration
- Attempts to keep a specific individual from getting to an administration
- Attempts to disturb administration to a particular framework or individual. A DoS assault could be propelled at any layer of impromptu system.

6. Defense Mechanisms to DoS Attacks

Protection components [18] to DoS assaults are arranged into two general classifications: neighborhood and worldwide. As the name proposes, neighborhood arrangements can be executed on the unfortunate casualty PC or its nearby system without an untouchable's participation. Worldwide arrangements, by their very nature, require the collaboration of a few Internet subnets, which regularly cross organization limits. A. Neighborhood Solutions Protection for individual PCs falls into three zones.

- Local Filtering: The timeworn transient arrangement is to endeavor to stop the penetrating IP bundles on the neighborhood switch by introducing a channel to identify them. The hindrance to his answer is that if an assault sticks the unfortunate casualty's neighborhood

coordinate with enough traffic, it likewise overpowers the nearby switch, over-burdening the sifting programming and rendering it inoperable.

- Changing IPs: A Band-Aid answer for a DoS assault is to change the unfortunate casualty PC's IP address, along these lines discrediting the old location. This activity still leaves the PC defenseless in light of the fact that the assailant can dispatch the assault at the new IP address. This choice is pragmatic in light of the fact that the present sort of DoS assault depends on IP addresses. Framework directors must make a progression of changes—to area name administration passages, steering table sections, etc - to lead traffic to the new IP address. When the IP change—which takes some time—is finished, all Internet switches will have been educated, and edge switches will drop the assaulting parcels.
- Creating Client Bottlenecks: The goal behind this methodology is to make bottleneck forms on the zombie PCs, restricting their assaulting capacity. B. Worldwide Solutions Clearly, as DoS assaults focus on the insufficiencies of the Internet overall system, neighborhood answers for the issue become purposeless. Worldwide arrangements are better from an innovative stance.
- Improving the Security of the Entire Internet: Improving the security of all PCs connected to the Internet would keep assailants from discovering enough helpless PCs to break into and plant daemon programs that would transform them into zombies.
- Using Globally Coordinated Filters: The methodology here is to avoid the gathering of a minimum amount of assaulting bundles in time. When channels are introduced all through the Internet, an injured individual can send data that it has recognized an assault, and the channels can quit assaulting bundles before along the assaulting way, before they total to deadly extents. This technique is viable regardless of whether the assailant has just caught enough zombie PCs to represent a danger.
- Tracing the Source IP Address: The objective of this methodology is to follow the interlopers' way back to the zombie PCs and stop their assaults or, stunningly better, to locate the first aggressor and take lawful activities.

In the event that following is done speedily enough, it can prematurely end the DoS assault. Getting the aggressor would dissuade rehash assaults. In any case, two assailant procedures block following; IP satirizing that utilizes produced source IP addresses, and The progressive assaulting structure that segregates the control traffic from the assaulting traffic, successfully concealing aggressors regardless of whether the zombie PCs are recognized. Point of this assault is to over-burden the server's data transfer capacity and different assets.

7. techniques for mitigating DoS attacks in MANET

A. Utilizing Protection Nodes The creators [24] have chosen a hub called security hub in a system. When a DDoS assault has been identified, the far fetched traffic will be sent to the security hub. The injured individual will work as common and it is normal that the assailant will stop the pointless endeavors after a specific length of assaulting time. For the choice of security hub, they have actualized the various leveled organize engineering in which the hubs are separated into numerous dimensions dependent on their significance. Lower level hubs are utilized to secure abnormal state hubs. Specifically, each lower level hub is doled out as its insurance hub called goal assurance hub or Local Protection Node (LPN). They protect the objective of DoS assaults. A neighbor of a similar dimension will be chosen as security hub for the most reduced dimension hubs. In this plan, when an assault course is made, the hub that is the main jump from the source hub will be doled out as a security hub called Remote Protection Node (RPN) which screens the assault source hub. In the event that the source hub is distinguished as a pernicious one, RPN drops the bundles from this hub. They have embraced three-advance handshake approach for choice of LPN by message correspondence.

- The larger amount hub sends the LPN question parcel (LPNREQ) to the hubs of its neighbor lower level. When the solicitation is gotten, neighbor hub's crisp labels are disconnected. At that point subsequent LPNREQ bundles from different hubs won't be acknowledged.
- The beneficiaries send an affirmation bundle (LPNACK) back to the sender. This PNACK message empowers that the recipient advises the sender that it is happy to fill in as the LPN; and the succession of the LPNACK messages enables the sender to settle on a choice. The maker of the primary got LPNACK parcel is chosen as the LPN.
- The ensured hub will send a LPN affirm (LPNCFM) message. The LPN hub channels all the malevolent bundles in the rush hour gridlock whose goal is the person in question. At that point Attack Notification Message (ANM) is sent to the unfortunate casualty right away.

Next, the unfortunate casualty sends an Attack Information Message (AIM) to RPN. At that point RPN channels all the assaulting bundles at source side. The upside of this methodology is cost of overhead of the framework is low and the impediment is organizing hubs into various dimension may prompt starvation to low dimension hubs. Additionally essential properties of a MANET may upset.

8. Conclusion:

We have proposed a mark based DoS relief framework for versatile impromptu systems. The framework characterizes an amusement wherein forwarders will probabilistically confirm parcels got for sending, and thus will get an opportunity to drop terrible bundles sent by assailants. We have figured various types of the diversion for various system situations, and dissected the relating result, viability, and Nash harmony properties. We have demonstrated that the diversions can instigate valuable DoS alleviation impacts. It is additionally appeared key amusement parameters, for example, the punishment for sending a terrible parcel without confirmation, can influence the likelihood that a hub will check a got bundle.

References

1. Akella, A. and A. Bharambe (2003). Detecting DDoS Attacks on ISP Networks. In ACM SIGMOD/PODS Workshop on management and processing of data streams (MPDS) FCRC.
2. Antonio, Challita (2005). A Survey of DDoS Defense Mechanisms; Department of Electrical and Computer Engineering American University of Beirut.
3. Biswas K. and Md. Liaqat Ali (2007). Security Threats in Mobile Ad Hoc Network. Master Thesis, Blekinge Institute of Technology, Blekinge.
4. Douligeris, C and A. Mitrokotsa (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 2004, pp. 643–666. Garber, L (2000). Denial-of-service attacks rip the internet. IEEE Comput., Volume 33, pp. 113-123.
5. Gavrilis and D. Gavrilis (2005). Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features, Computer Networks48 (2) (2005), pp. 235–245.
6. Geng, X.J. and A. B. Whinston (2000). Defeating Distributed Denial of Service Attacks. IT Professional, Vol. 2, No. 4, 2000, pp. 36-41.
7. Gowadia and V.Gowadia (2005). PAID: A probabilistic agent-based intrusion detection system, Computers and Security24 (7) (2005), pp. 529–545.
8. Han, B, H. H. Fu, L. Lin and W. Jia. Efficient Constructionof Connected Dominating Set in Wireless Ad Hoc Networks. IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Fort Lauderdale, 25-27 October 2004, pp. 570-572.
9. Hwee-Xian, Tan and K.G. Winston Seah (2005). Framework for Statistical Filtering Against DDOS Attacks in MANETs. IEEE, Proceedings of the Second International Conference on Embedded Software and Systems.
10. Laurens, V (2006). Detecting DDoS attack traffic at the Agent Machines. Canadian Conference on Electrical and Computer Engineering. CCECE'06, Ottawa, pp. 2369-2372.
11. Li, Q, E-C. Chang and M. C. Chan (2005). On the Effectiveness of DDoS Attacks on Statistical Filtering. Proceedings of the 24th Annual Conference of the IEEE Communications Society (INFOCOM), Miami; Mar 13-17.
12. Li-Chiou, Chen, Thomas A. Longstaff, and Kathieen M. Carley (2004). Characterization of defense mechanisms against distributed denial of service attacks. Computer & Security Volume 23, pp. 665-678.
13. Meghna, Chhabra., Brij Gupta and Ammar Almomani (2013). A Novel Solution to Handle DDOS Attack in MANET. Journal of Information Security, pp. 165-179.
14. Murthy, C. S. R. and B. S. Manoj (2004). Ad Hoc Wireless Networks Architectures and Protocols. Prentice Hall Communications Engineering and Emerging Technologies Series, Pearson Education, Upper Saddle River.
15. Piskozub, A (2002). Denial of Service and Distributed Denial of Service Attacks. Proceedings of the International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science, pp. 303-304, Lviv-Slavsko.
16. Sarkar, S. K. (2008). Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications. Auerbach Publications, Boca Raton, 2008

