ISSN: 2348-2079

Volume 3 Issue 8

International Journal of Intellectual Advancements and Research in Engineering Computations

AN ADEPT METHOD TO DETECT AND TRACEBACK DDoS ATTACKS IN WIRELESS NETWORKS USING PACKET FLOW ANALYSIS

[1]S.Sathishkumar, Research Scholar, Annamalai University, Chidambaram, Tamilnadu, India.

[2]A.Senthilkumaar, Professor, Annamalai University, Chidambaram, Tamilnadu, India.

Abstract

The recent past has entered into an era of implementing wireless networks for the better beneficiary outcomes when compared to that of traditional wired networks. The support that the wireless networks provide in connectivity, availability of resources and cost wise comparisons has made them more popular. However there have been certain limitations to the open nature of the wireless framework in terms of security and confidentiality. Better the security measure yields an even stronger attack. The most prominent attack of the wireless network is the Denial-of-Service attack. These attacks tend to alter the legitimate communication between the service provider and the requester, by sending unwanted and meaningless data into the medium. Traceback mechanisms try to identify andblock the attackers from proceeding. Evaluation of these mechanisms depends on the level of how well they try to keep the attackers beyond the normal functionalities of the wireless network. This paper is dedicated to estimate the variations in the normal and attack traffic in the wireless networks.

Index terms: Network security, Trace back, DoS attacks

Introduction

The internet most preferable server to all requests and queries has progressed into a greater altitude. The wireless networks offer a wide range of services to almost all users who possess internet connectivity. Wireless networks eliminate the difficulties of the wired networks as they are simplified in their architecture still obeying the standards of the IEEE. These networks are implemented in almost every core in today's world. Efficient communication between the users should be noted among legitimate and the supposed members of the network. While the wireless sensor network is prone to a higher extent of attacks than the traditional network structures, they have a strong reason to be applied in major applications.

The Denial of Service attacks in the wireless sensor networks are the notable attacks that need to be contained. There exists a certain limit of data to be transmitted through a medium between the legitimate users. This transfer of data is unaffected if the flow is within the competence level of the medium. But in case of intrusion of a compromised user or an attacker (zombies), they try to flood the normal traffic with unlimited packets of data into the medium. The flooding of data packets causes the medium to be congested leading to the denial of service to the intended users.

Carrier Sense Multiple Access/ Collision Detection mechanisms are some of the methodologies proposed to enable the nodes to avoid the congestion and to utilize the medium with absolute functionality. The attackers invert the entire concept to their advantage to keep the medium busy until the nodes suspend the transmission of the packets.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

When the attacker sends in the meaningless packets into the medium, the original user would try to sense the medium and finds it to be busy. The node would mistake that another legitimate user is under transmission and thus keeps waiting until the medium is freed.

Hence in order to preserve the security of the network and its process, several algorithms have been proposed to spot the network being attacked, recognizing the attacker and retrieving his details and thus preventing the network from the damage.

Related Technologies

Proposed trace back mechanisms have been trying to eradicate and mitigate the denial-of service attacks but have not achieved the success level. Trace back is carried out by backtracking the distance which the packets came to the source. This has not been successful due to the reasons such as improper and incomplete information on the packets. The nodes which generate the attack packets are either compromised or spoofed (the original IP address is changed). In case of a spoofed address, the respective node details are completely invisible to the trace back algorithms. On the other hand, if it is a compromised node, the network itself would authorize the transmission.

To perform a trace back function, the information on the path which the packet travelled towards the destination or victim node is required. The information has to be updated in the packet by the markings of the routers it passed. This methodology one of the challenging trace back mechanisms called as packet marking is classified into two categories namely, Probabilistic Packet Marking and Deterministic Packet Marking. The former required the addition of the IP address of every router the packet crossed which is quietly impractical in wireless networks. The packet's space is limited and cannot be loaded with all the router information. The packets of internet are supposed to travel through a long distance from the source to destination via a number of routers. There is a high chance for the information of the last router replacing the initial routers. Moreover there is no surety for believing that the information recorded in the attack packets are true enough to trace back right to the attacker. The availability of the information is quite inconsistent or inadequate in most situations.

This paper discusses the methodologies of the analyzing the threshold values of normal traffic and attack traffic. The traffic defines the number of data packets that would travel in the medium during the communication of nodes at a regular time, at peak time and during a congested time. This level is called as the threshold value which denotes the permitted level of traffic at the different time zones and if the packets flow is much higher than the threshold value, the network is alarmed about the attack and the defensive mechanisms are activated either to detect the attacker node or block the data flow of the attacker. The entropy is the metric which represents the data flow in the medium. The major drawback of this method is the difficulty in differentiating between the congested traffic and the attack traffic. The high rate of the false negatives limits the implication of these methods.

The entropy metric is determined by certain calculations based on the probability of the input packet flow in the respective time zone and between the stated destinations. The calculation may involve the details of the IP address of the destinations, the routers information and details about the path in between. After the initial measurements and determination of the entire threshold values at various traffic time (normal, congested and attack), the network commences its function. Then the medium is continually observed with respect to the rate of traffic flow in the medium. The packet flow analysis would estimate the corresponding value of the variations every now and then. Estimated packet flow rates are subjected to comparative studies with the threshold values. These comparisons would explain the level of traffic and alarm the network under attack. When the calculated value denotes the considerable increase than the normal and legitimate transmission of the data packets in the medium, the defensive mechanisms are activated.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

The routers which sense the incremented values are made to block the traffic and then its upstream routers are notified about the attack. Immediate routers above in the path would trace back to the source of the attack. This detection and trace back method is based on the estimated packet flow.

Limitations of Existing Technologies

The evaluation of the entropy values requires the entities such as the IP address of the destination and the path every packet selects to reach the victim in a wireless network.

The wireless networks have practically no bounds, and the open nature makes the security mechanisms an exigent task to be designed and implemented. In the case of a wired network, the number of nodes, the platforms and the environment is known to everyone. Hence tracking the attacker in the predefined network constraints is an easier task for the detection and trace back algorithms. The same ideology does not apply in the wireless networks where there are no criteria other than a network connection to be a part of the network. The user possessing the right user id and the password could possibly gains access to the network.

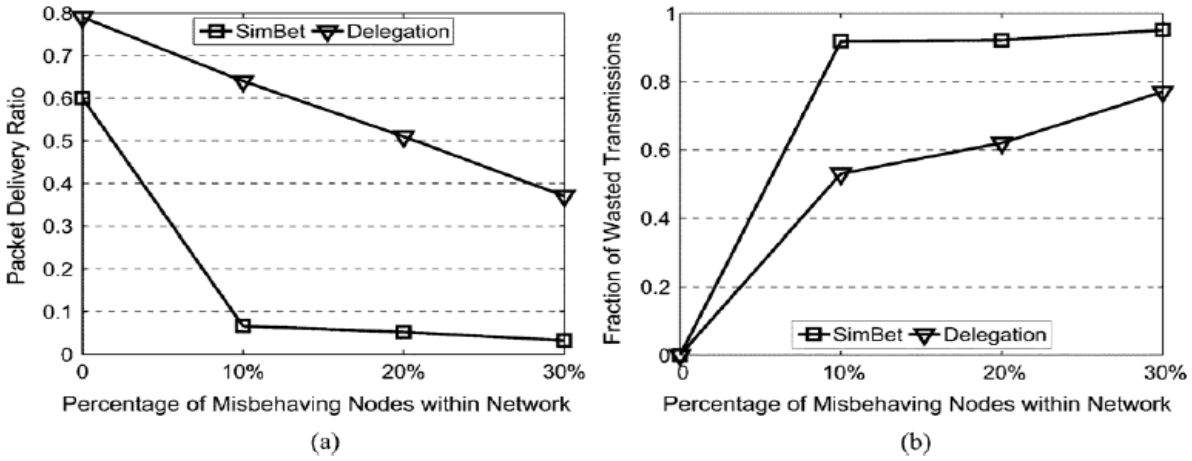
Analyzing the concepts of security enforcements in wireless networks, certain changes have to imply on the specific concepts in the mentioned packet flow analysis. The wireless networks are nodes which have no physical links established in between and outside the network. The boundaries of the network are framed by means of the farthest routers which allow the entry of packets towards the destination. Thus there can be external routers considered to the gateway and act as the virtual boundary for a wireless network. The estimation of the threshold values on incoming packet flow could be carried out in these external routers.

The determination of the entropy threshold values and the comparison of the packet flow during transmission require repeated computations. Computations need notable time and executions which have immediate effects over the performance of the defensive mechanism. The mechanism is effective if and only if all the routers are subjected to the packet flow analysis and obtaining the entropy values. The number of routers and nodes in wireless networks cannot be fixed. This poses a serious threat to the application of the methodology. The flexibility nature of the wireless networks need to be assigned with limits for better efficiency. Since the time required for computations are high and the number of computations are greater than that of wired networks, they need a better strategy.

Denial of Service attacks has evolved to evade the defense strategies and detection algorithms. The current attacks in today's applications are capable of falling low and within the estimated threshold value. The attacks are coordinated and distributed in most cases of the attacks. Low rate DoS attacks are the best example for escaping from detection algorithms such as entropy variations.Disruption Tolerant Networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Due to a lack of consistent connectivity, two nodes exchange data only when they move into the transmission range of each other (which is called a *contact* between them). Thus, DTN routing usually follows "store-carry-forward;" i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards the packet.

In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks. Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets. To demonstrate this, we simulate the effects of routing misbehavior in two popular DTN routing algorithms, SimBet and Delegation based on the Reality trace. SimBet is a forwarding-based algorithm where a packet only has one replica. Delegation is a replication-based algorithm where a packet may have multiple replicas.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com



When 30% of the nodes with higher connectivity are misbehaving, SimBet only delivers 30% of the packets whereas Delegation only delivers 40%. Moreover, 95% of the transmissions in SimBet and 80% in Delegation are wasted since the packets are finally dropped by misbehaving nodes. Although Burgess *et al.*studied the effects of packet dropping on packet delivery ratio, they did not consider the wasted transmission (bandwidth) caused by dropping. Therefore, it is extremely important to detect packet dropping and mitigate routing misbehavior in DTNs.

Proposed Methodology

The architecture of the wireless networks is assigned with Gateway Routers which are the external routers acting as the boundary.

The number of nodes is limited to an extent and divided into various smaller networks. Reducing the computational time of the packet flow entropy values is achieved by compressing the information using lossless compression techniques. After compression, the information used for evaluation would be smaller in size and easier to compute. The packet flow analysis starts from the Gateway routers to the internal routers. After the commencement of the transmission of data packets, traffic flow is often checked with the threshold values. If the analysis proves that the network is under attack, the defense mechanism is activated.

MARKING PHASE

Routing Security: Our model only evaluates the security of the routing itself. While routing may be accomplished without authentication, this does not obviate the need for end-to-end authentication and confidentiality mechanisms. We also ignore any attacks on the applications themselves, such as spoofing requests that cause legitimate nodes to flood other legitimate nodes with unneeded traffic. Knowledge: We distinguish between weak and strong attackers. Nodes are chosen to be weak attackers uniformly at random to simulate an opportunistic attack in real wired or wireless networks. Such opportunities may arise due to mobility, i.e., passing an infected node, or chance weakness, seen in the propagation of botnets. In contrast, strong attackers have knowledge of the complete network topology, which is likely to be more information than any node would have in practice. These two versions of our attacker

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

provide points of reference for what is possible for attackers in a DTN. We expound upon the analysis of weak and strong attackers below.

Mobility: An attacker can follow any mobility pattern and attack all nodes that move within wireless range, or she can remain permanently within range of one node in the network. We call the latter approach a parasite attack; it is the most effective use of the attacker's resources.

Attack types: There are two forms of the parasite attack: node corruption and tailgating. Under node corruption, an attacker has completely taken over a node and can command it to create and drop packets at will. In some settings, this attack can include physical destruction of the target node. The tailgating attacker is external to the uncorrupted node, but can arbitrarily give it extra packets to forward, spoof outgoing packets, or selectively interfere with the delivery of packets during connection opportunities. The tailgating attacker is as powerful as node corruption since the effect of both is identical.

Given this security model, a number of attacks are possible. To simplify analysis, we focus on a set of actions that are fundamental to any attack. These four actions are detailed below

in the context of DTN transfer opportunities: exchanging packets, exchanging routing tables, and exchanging acknowledgments. When a network is restricted to authenticated, authorized participants, one would expect these attacks are avoided or at least attributable to some entity.

• Dropping all packets

• Flooding of packets

• Routing table falsification

• Counterfeit acknowledgments of delivery

3.3.4 Contact Records

The two nodes also exchange their current vector of buffered packets (as a step of contact record generation). In this way, one node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted by and , respectively. It also knows the two sets of packets the other node sends and receives in the previous contact, which are denoted by and a misbehaving node may drop a packet but keep the packet ID, pretending that it still buffers the packet.

The next contacted node may be a better relay for the dropped packet according to the routing protocol, which can be determined when the two exchange the destination (included in packet ID) of the buffered packets. In this case, the misbehaving node should forward the packet to the next contacted node, but it cannot since it has dropped the packet. Thus, the next contacted node can easily detect this misbehavior and will not forward packets to this misbehaving node.

3.3.5 Witness Node

Detection: To detect the inconsistency caused by misreporting, for each contact record generated and received in a contact, a node selects random nodes as the witness nodes of this record, and transmits the summary of this record to them when it contacts them. It selects the witness nodes from the nodes that it has directly contacted. Here, the nodes contacted a long time ago are not used since they may have left the network.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

Alarm: After detection, the witness node floods an alarm to all other nodes. The alarm includes the two inconsistent summaries. When a node receives this alarm, it verifies the inconsistency between the included summaries and the signature of the summaries. If the verification succeeds, this node adds the appropriate misreporting node into a blacklist and will not send any packets to it. If the verification fails, the alarm is discarded and will not be further propagated. A misreporting node will be kept in the blacklist for a certain time before being deleted.

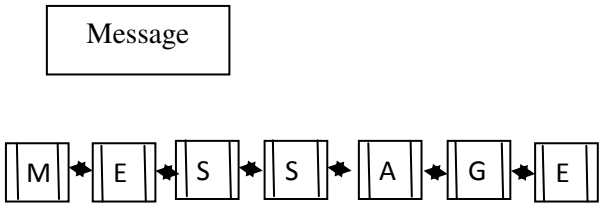
A node deletes the record that it generates in a contact after the contact has been purged out of its report window, probably after a few contacts. It deletes the records received from the contacted node right after this contact, since these received records are only used to check if the contacted node has dropped packets recently. The witness node should keep its collected record summaries for a long enough time to detect misreporting. For simplicity, our scheme uses a time-to-live parameter, which denotes the time for the collected summaries to be stored before being deleted

Black List

To mitigate routing misbehavior, we try to reduce the number of packets sent to the misbehaving nodes. If a node is detected to be misreporting, it should be blacklisted and should not receive packets from others. We cannot simply blacklist it because it is dropping packets, since a normal node may also drop packets due to buffer overflow. In the following, we focus on how to mitigate routing misbehavior without affecting normal nodes too much when misbehaving nodes do not misreport.

Our basic idea is to maintain a metric forwarding probability (FP) for each node based on if the node has dropped, received and forwarded packets in recent contacts, which can be derived from its reported contact records. The nodes that frequently drop packets but seldom forward packets will have a small FP and will receive few packets from others. Our scheme borrows ideas from congestion control to update FP. More specifically, it combines additive increase, additive decrease, and multiplicative decrease to differentiate misbehaving nodes from normal nodes.

A message is the carrier of information to and fro in the network. Each message is broken into a number of smaller packets for ease of transmission. The new approach involves the packet marking techniques right at this phase. After the packets are divided into a number of smaller packets, each packet is marked by the address or identity order of the next packet. Each packet is marked by the address of its preceding and succeeding packet. It forms a loop of packets. The Gateway Router checks for the connectivity of packets to be sent into the closed sub network. Packets other than the identity of connection are discarded from the GRs. Packets other than the whole message cannot possess an identifier, and other packets from different other legitimate systems possess different values of ids.



The number of packets to be split is determined by the size of the algorithm. Each packet header comprises of the source and destination address. In this methodology, additionally the links to the next packet and preceding packets are marked into the IP header. The GRs are supposed to check the entering packets with a confirmation of grouping a whole message. Extra packets are confronted to be removed at the bay itself. Limited capacity of bandwidth cannot be misused with meaningless packets of intruders in this scheme.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

Algorithm

AT NODE LEVEL:

```
CLUSTER()
        FOR EACH GATEWAY ROUTER ASSIGN()
                NODE1()
                NODE2()
                    :
                NODEN()
```

AT TIME OF COMMUNICATION:

```
MESSAGE(INFO)
        MARK()
                SPLIT()
        {               PKT(1)+PKT(2)+…PKT(N)
        }
                LINK()
        {
        PKT(1) TO PKT(N)
        }
                PATH(OPTIMAL CONDITION)
                DESTINATION(INTENDED)
AT NODE LEVEL:

CHECK()
        ID OF PKT(1) TO PKT(N)
VERIFY()
        ENTRY OF SURPLUS PKT(S)
DISCARD()
        SURPLUS PKT(S)
TRACEBACK()
```

Comparison of the threshold values too starts at the Gateway Routers. The first step of the defensive mechanism is to block the traffic at the GR itself. If the routers nearer to the victim node are compared and found to be under attack, the upstream routers are forced to traceback and report the source. The proposed architecture is as follows.

Let us consider an organization with n number of systems implemented for various purposes of administration, accounting, computation, and display. There are nodes which need to be secured in order to conserve the integrity of the network. Resources of the organization have to be rightly conserved without the exposure to external users. No part of the network can be accessed directly by an external user.

The network can implement the proposed ideology for achieving security. The architecture of the wireless networks is assigned with Gateway Routers which are the external routers acting as the boundary. The Gateway Routers (GR) is the only entry and exit points to the sub network of systems. These sub networks form the protected network

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

framework of the organization. The programs for analyzing the flow of packets is employed in GRs. Subjecting these sub networks into analysis enhances the performance, eliminating the need of defining standard protocols in higher levels of abstractions.

The number of nodes is limited to an extent and divided into various smaller networks. Reducing the computational time of the packet flow entropy values is achieved by compressing the information using lossless compression techniques. After compression, the information used for evaluation would be smaller in size and easier to compute. The packet flow analysis starts from the Gateway routers to the internal routers. After the commencement of the transmission of data packets, traffic flow is often checked with the threshold values. If the analysis proves that the network is under attack, the defense mechanism is activated.

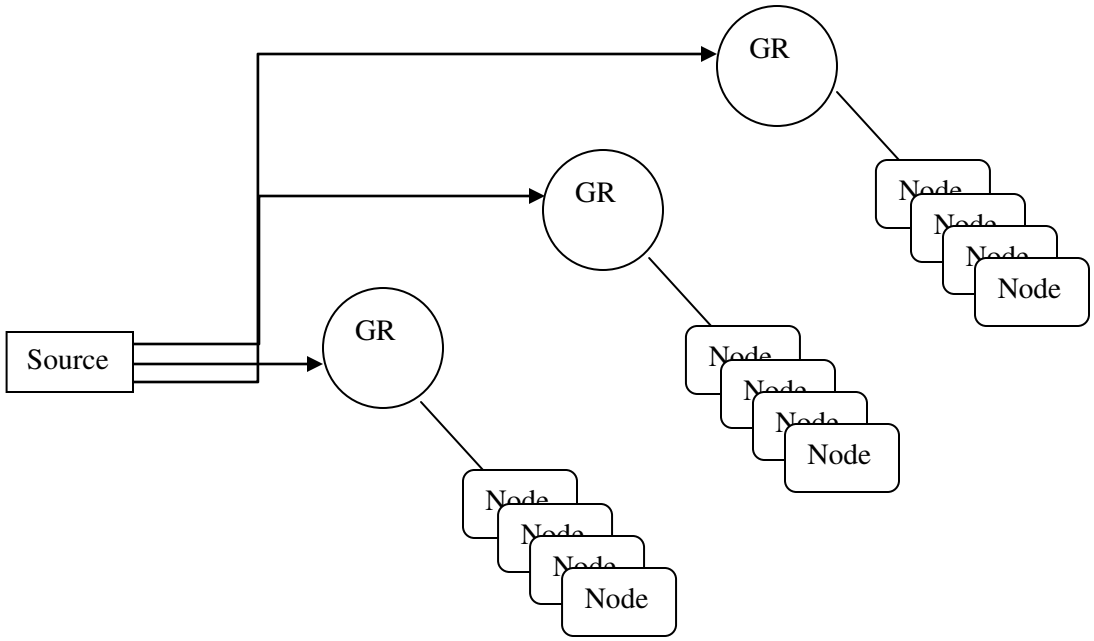


Fig: Architecture of Gateway Routers

The exceptional cases where the attacker is aware of the defensive mechanism present in the network, the attack packets would be of low rate to appear as normal packets or distributed.In either case the detection would be difficult as the entropy metrics wouldnot report a hike and act as a legitimate traffic of packet flow. To overcome these limitations, the determinations of the entropy values should be assisted with the mechanisms for detecting low rate DoS attacks and distributed DoS attacks. The comparison of entropy metric of normal and congested networks is followed by the detection of low level DoS attacks when the traffic flow is altered. Elimination of reporting congested legitimate traffic is achieved by proper analysis for stated amount of time.

Detection algorithms of low rate DoS attacks would involve more computations and as the whole this mechanism would require a greater time for reporting. The packet flow analysis is optimized by introducing faster computation techniques. The incorporation of the additional mechanism would enhance the security level of the wireless networks. Reduction in the computation time is balanced by the time needed for the additional algorithm and the concept of parallel processing helps the mechanism to end faster. Further simplifications on the computations and confiscating the number of computation processes would yield a better execution time and detects the attacker faster.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

Conclusion

This paper comprises of a method to detect and traceback the attacker of the new trend. Irrespective of the evasion activities, this method identifies the network under attack and tends to trace the attacker to his location. The wireless networks are prone to easier attacks and this method will prove to be an effective defense mechanism over all kinds of Denial of Service attacks. Unfortunately, there is so far no mechanism that can completely prevent the attack of peers being compromised. We plan to engage in a study of attacks made via anonymous operations, and develop corrective and preventive methods as a part of trust building and trust management research.

References

[1] C. Schleher, *Electronic Warfare in the Information Age*. Artech House,1999.
[2] R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an on-off jamming situation as a dynamic game," *IEEE Trans.Commun.*, vol. 48,no. 8, pp. 1360-1373, Aug. 2000.
[3] D. Wood and J. A. Stankovic, "Denial of service in sensor networks,"*IEEE Comput.*, vol. 35, no. 10, pp. 54-62, 2002.
[4] R. Negi and A. Perrig, "Jamming analysis of MAC protocols," Carnegie Mellon technical memo, 2003.
[5] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proc. USENIX Security Symp.*, pp. 15-28, 2003.
[6] Wood, J. Stankovic, and S. Son. "JAM: a jammed-area mapping service for sensor networks," in *Proc. IEEE Real-Time Syst. Symp.*, pp.286-297, 2003.
[7] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 29-30, 2003.
[8] J. M. McCune, E. Shi, A. Perrig, andM. K. Reiter, "Detection of denialof-message attacks on sensor network broadcasts," in *Proc. IEEE Symp.Security Privacy*, 2005.
[9] W. Xu *et al.*, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM Int'l. Symp. Mobile Ad Hoc Netw.Comput.*, 2005, pp. 46-57.
[10] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc IEEE INFOCOM*, May 2007.
[11] Q.Huang, H.Kobayashi, and B.Liu. "Modeling of distributed denialof service attacks in wireless networks," in *IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003*
[12] L.Sherriff, "Virus launches DDoS for mobile phones," [Online]. Available: http://www.theregister.co.uk/content/l/12394.html
[13] M. Acharya and D. Thuente, "Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks," in *Proc.OPNETWORK-2005 Conf.*, Washington DC, USA, Aug. 2005.
[14] Y.Zhang, W.Lee, and Y.-A.Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *in ACM J. Wireless Net., vol. 9, no. 5, Sept.2003, pp. 545-56.*
[15] A.B.Smith, "An examination of an intrusion detection architecture for wireless ad hoc networks," in *5th National. Colloq. Inf. Syst. Sec.Education*, May 2001.
[16] O.Kachirski and R.Guha, "Intrusion detection using mobile agents inwireless ad hoc networks," in *Knowledge Media Net., Proc. IEEE Wksp.*,July 10-12, 2002, pp. 153-58.
[17] W.Xu et al, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. 2004 ACM Wksp. Wireless Security*,2004, pp.80-89.
[18] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE iNFOCOM, Mini-Conf.*, 2007.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com