ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

# Cache Consistency and IDS for Handling Attacks in Routing Ad-hoc networks

P.Preethi Monolin[#1], Dr.J. Amutharaj[*2]

P.G Student, Dept. of M.E CSE, Alpha college of Engineering, Chennai, Tamil Nadu, India[# 1]

Professor & Head, Dept. of ME CSE, Alpha College of Engineering, Chennai, Tamil .Nadu, India[* 2]

**ABSTRACT:** Ad-hoc networks are composed of autonomous nodes that are self-managed without any infrastructure. Due to their dynamic topology, wireless Ad-hoc networks are vulnerable to Denial of Service (DoS) attacks—an instance of a resource depletion attack, with battery power as the resource of interestw. This type of attack is termed as "Vampire" attacks. Such attacks are encountered in two phases: Topology Discovery and Packet forwarding phase where a cache consistency scheme is proposed. In the topology discovery phase, nodes are discovered by the neighbors by building a tree of Neighbor relationship and Grouping membership used for addressing and routing. The PLGP (Parno, Luk, Gaustad, and Perrig) routing protocol which is responsible to perform the no-backtracking property is enhanced with the Ad-hoc routing protocols such as DSR (Dynamic Source Routing) and AODV (Ad-hoc On- demand Distance Vector) such that it ensures malicious node prevention during the packet forwarding phase. The topology is discovered along with the attack description by means of Intrusion Detection Scheme such that attacker has minimum possibilities to get involved in the succeeding packet forwarding phase. However, the PLGP with attestation of a history table is enhanced with Ad-hoc routing protocols depending upon the attack identified in the previous phase. Finally, a performance evaluation statistics is compared with the existing results.

**KEYWORDS –**Ad-hoc networks, DoS attacks, routing protocols, resource depletion, Detection schemes

## I. INTRODUCTION

Ad-hoc wireless networks are composed of autonomous nodes that are self-managed without any infrastructure. Ad-hoc networks are suitable for areas where it is not possible to set up an infrastructure, they provide the connectivity by forwarding packets over themselves. In this way, ad-hoc networks form a dynamic topology such that nodes can easily join or leave the network and nodes can directly communicate with other nodes in its range at any time, where mobility is considered. It is a decentralized network of nodes with radios, possibly mobile, sharing a wireless channel and asynchronously sending packets generally over multi hops. Ad-hoc network is also known as Independent Basic Service Set (IBSS) configuration. Logically, this configuration is analogous to a peer-to-peer network in which no single node is required to function as server. Ad-hoc WLANs include a number of wireless stations that communicate directly without an access point (AP) or any connection to a wired network.

Ad-hoc routing protocols can be classified as either proactive or reactive depending on the method used to discover and maintain routes. Effective routing protocols are needed to establish communication paths between nodes, without causing excessive control traffic overhead or computational burden on the power constrained devices. The Proactive Routing protocols exchange routing information periodically and on topology changes. In this case, it is not necessary to have an up-to- date route to all other nodes. Whereas, the Reactive Routing protocols set up routes to nodes they communicate with and these routes are kept alive as long as they are needed. Hybrid Routing is the combinations of proactive and reactive protocols, where nearby routes (for example, maximum two hops) are kept up-to-date proactively, while far-away routes are set up reactively, are also possible and fall in the category of Hybrid Routing protocols

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

The prerequisite of a routing service in Ad-hoc environment is a distributed mechanism for the discovery and maintenance of routes. Malicious nodes aim to deliberately disrupt the correct operation of the routing protocol, denying the network service if possible. Both data packets and control packets, as used by the routing protocol, are vulnerable to attacks. Some of the examined attacks encountered during the routing of data packets are discussed: Blackhole Attack also called as a packet drop attack occurs when a router which is supposed to relay packets; discard them. A malicious node falsely advertises good paths to a destination node during the route discovery process but drops all packets in the data forwarding phase. When an adversary receives packets at one point in the network, "tunnels" them to a different point in the network and then replays them from this point. Two nodes use an out-of-bound channel (e.g. a directional antenna) to forward traffic between themselves and enabling them to mount other attacks. Flooding Attack occurs when attacker exhausts the network resources such as bandwidth, consumes node's computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. The most common Link Spoofing Attack Malicious node advertises fake links with non-neighbors to disrupt the routing path. When the attacker records another nodes control messages and resends them later. It can be used to spoof another node or just disrupt routing, called as Replay Attack.

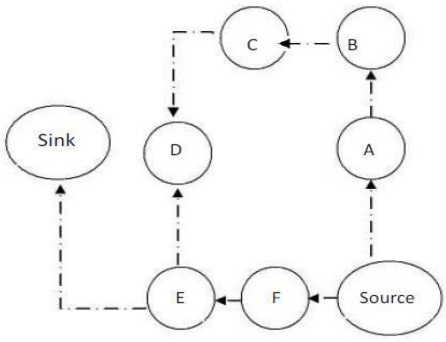


Fig. 1 Stretch attack

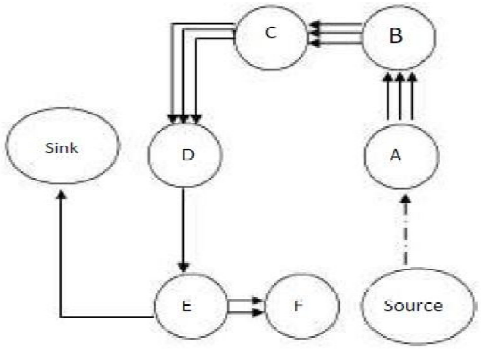


Fig. 2 Carousel attack

In this paper, two attacks are discussed and analyzed with the Intrusion Detection Scheme (IDS). Firstly, the Stretch Attack as shown in fig. 1 shows the attacker targets the source routing; an adversary constructs artificially long routes, potentially traversing to every node in the network. It is called as the Stretch attack since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. Secondly, the Carousel Attack where an adversary composes packets purposely introducing routing loops. It is called as the Carousel attack, since it sends packets in circles as shown in fig. 2. It targets source protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse at the same set of nodes. Finally, the Stretched Cycle Attack where effective malicious nodes can be configured in more than one way, involving in the network by damaging simultaneously the entire nodes in a group; here it is called the Stretched Cycle attack, the combination of both Stretch attack and Carousel attack. In this fig., Honest Node is dotted while malicious route is dashed. The last link to the sink is shared. An Honest node would exit the loop immediately from node E to sink, but a malicious packet makes its way around the loop twice more before exiting.

## II. RELATED WORK

In [1] a secured routing protocol is designed, implemented and evaluated. The central design parameter is to adopt a clean-slate approach and to design a new sensor network. The Recursive Grouping Algorithm is performed by merging

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

small groups repeatedly to form a larger group and then the nodes are labelled with their IDs as well as their resulting network addresses. At each stage of the grouping algorithm, the groups are assigned IDs that, along with their sizes can be authenticated using Grouping Verification Tree (GVT). At the completion of the grouping protocol, each node will have a unique network address, a routing table that maps variable length address and a merge table that will be used to secure each step of algorithm. At each stage of the grouping algorithm, the groups are assigned IDs that, along with their sizes can be authenticated using Grouping Verification Tree (GVT). At the completion of the grouping protocol, each node will have a unique network address, a routing table that maps variable length address and a merge table that will be used to secure each step of algorithm. If a legitimate node detects malicious behavior using the replication detection algorithm, then it uses the Honeybee recovery mechanism. Essentially, the legitimate node broadcasts a packet implicating the malicious node, and the other legitimate nodes revoke both nodes involved. By revoking both nodes, we limit the potential damage of a slander attack, since a malicious node can only revoke a single legitimate node before being revoked itself.

Whereas the DoS attacks can be prevented if the spoofed source IP address is traced back to its origin which allows assigning penalties to the offending party or isolating the compromised hosts and domains from the rest of the network as proposed in [2]. IP traceback mechanisms are based on probabilistic packet marking (PPM) have been proposed for achieving traceback in DoS attacks. This paper implements PPM with deterministic packet marking and logging or messaging based schemes resulting in spoofing of the marking field in the IP header by the attacker which can impede traceback by the victim. There is a trade-off between the ability of the victim to localize the attacker and the severity of the DoS attacks, which is here represented as a function of the marking probability, path length and traffic volume. The optimal decision problem is that the victim can choose the marking probability whereas the attacker can choose the spoofed marking value, source address and attack volume which can be expressed as a constrained minimax optimization problem, where the victim chooses the marking probability such that the number of forgeable attack paths is minimized. The attacker's ability to hide his location is curtailed by increasing the marking probability; however, the latter is upper-bounded due to sampling constraints.

In typical IP internets, the attacker's address can be localized to within 2-5 equally likely sites which render PPM effective against source attacks. In the deterministic packet marking, the source of a traffic flow is recovered by employing tracing information inscribed in the packet. Packet marking can be viewed as a form of "stateless logging" which emulates the capability of path recovery by router based information logging, without incurring the latter's state fullness and associated space overhead. Whereas, in the probabilistic packet marking each router probabilistically inscribes its local path information onto a traversing packet so that the destination node (i.e. victim of an attack) can be reconstruct, with high probability. This corresponds to probabilistically "sampling" the route undertaken by an attack using constant space in the packet header independent of hop count, which provides the key advantage over deterministic packet marking. In PPM, an attacker can forge a path that is equally likely as the optimal attack path by transmitting corrupted packets that reach the victim unmarked.

## III. OVERVIEW OF THE EXISTING MODEL

Strength of vampire is measured and determined by the ratio of network energy used in the beginning case to the energy used in the malicious case, i.e. the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remain constant. Safety from vampire attacks implies that the ratio equals to 1. The PLGP (Parno, Luk, Gaustad, Perrig) as discussed in [1] routing protocol is introduced with a clean-slate approach, considering the security and efficiency as the central design parameters. In order to ensure security in a routing protocol, it must incorporate three techniques: Prevention, Detection/Recovery and Resilience. The route setup in PLGP is done with the following goals:

**A.** Assigns an unique network address to each node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

Assume that Group G and G' decides to merge, then each node in G independently extends its network address by one bit based on:

$$R_i = \begin{cases} 0 & ID_G < ID_{G'} \\ 1 & ID_G > ID_{G'} \end{cases}$$

$$ID_{r=} \begin{cases} h(ID_G, |G| ID_{G'}, |G'|) & ID_G < ID_{G'} \\ h(ID_{G'}, |G'| ID_G, |G|) & ID_G > ID_{G'} \end{cases}$$

**B.** Populate each node's routing table

Here, each node in G records the neighbor from whom it heard about G' in its current routing table slot. Maintains Recursive Grouping algorithm and detect group deviations by Group Verification Tree (GVT). Based on the hash tree construction when two groups are merged initially verify each other's GVT.

**C.** Resilient forwarding

To achieve high availability of message delivery multi path forwarding is performed in route maintenance. The routing tables established during Recursive Grouping algorithm is extended with multiple next-hop nodes at each stage.

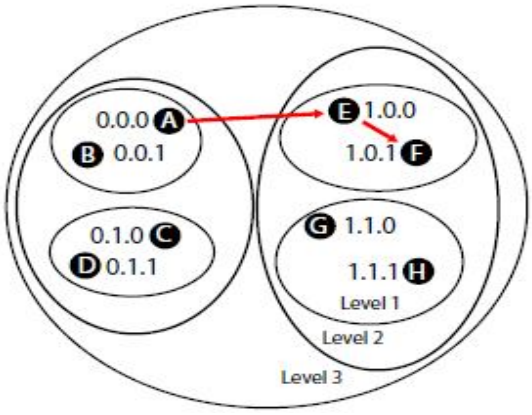


Fig. 3 Recursive Grouping outcome

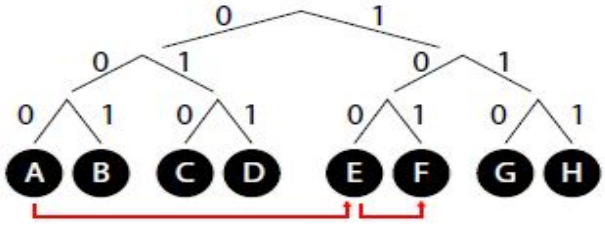


Fig. 4 Generation of Network address

The PLGP protocol can be modified to provably resist Vampire attacks during the packet forwarding phase. Thus PLGPa (PLGP with attestation of a history) protocol is introduced by Vasserman and Hopper [3] which encounters vampire's in two phases: Topology Discovery phase and Packet Forwarding Phase.

## IV. PROPOSED ATTACK HANDLING MECHANISM

A vampire attack is a composition and transmission of messages which causes more energy in the network relatively compared with an honest node transmitting a message of identical size to the same destination, using different packet headers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

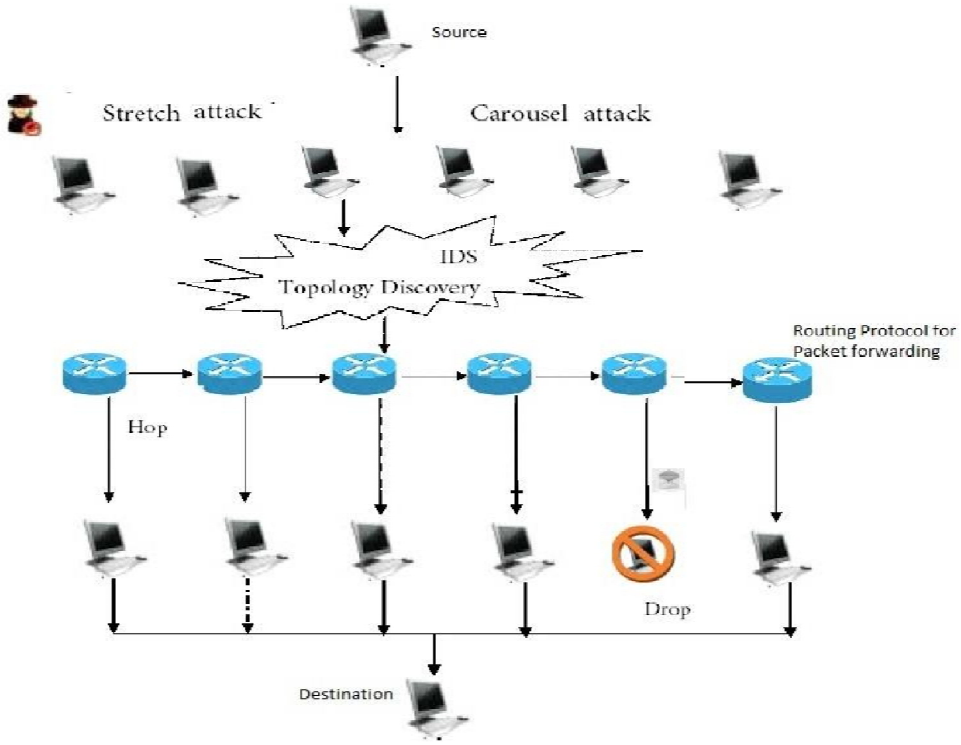


Fig 5. Proposed System architecture

**A. Attacks Description**

At the initial stage such type of attack is identified by the IDS mechanism. The HN certificate is authorized to all nodes in the network when a packet is to be transmitted. At the prior case, the possibility that the source itself is a Vampire can be identified at this stage and the packet is discarded.

**Topology Discovery Phase:** In the Ad-hoc environment one of the challenges during a packet transfer is to initially determine the topology such that the optimal route path is identified. Here, source routing is done by broadcasting RREQ (Route Request) messages to its neighbor nodes. The collected RREP (Route Reply) messages are then used to form the Neighbor-Relationship and Grouping membership, such that an optimal path is identified with multiple possibilities to ensure resilient forwarding of packets.

As shown in fig. 6 the comparison with number of nodes are sited with malicious behavior. Though the possibility of an intruder is high in an Ad-hoc network the cases of link failure resulting in packet drop is 99% reduced since node cache is efficiently updated periodically when a new node enters a network. The Honest node preserves its cache path to reach the destination in case of the expires TTL (Time To Live) then cache is updated to all its neighbor position nodes for awareness.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

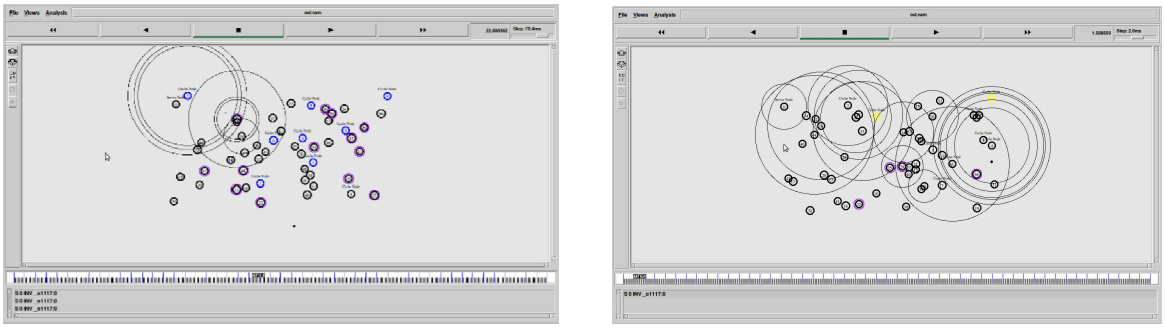

Fig 6. Resilient packet forwarded within 50 node wireless network in the presence vampire

**Packet Forwarding Phase:** When the source itself is an attacker it can be identified by IDS that certifies HN provides a Static ID, to each node. In case, the attacker involves at the intermediate node or a packet is found to be received more than once to the same node, then the PLGPa with traced path is verified. The DSR is enhanced by maintaining the cache consistency mechanism at each node such that multi-path forwarding is possible during link failure. A hold-down timer is attached along with the packet to ensure arrival at the Sink without loop.

### B. Intrusion Detection Scheme (IDS)

The proposed system consists of the following main functional components:

1. An Intrusion Detection Scheme is proposed by extending PLGPa protocol during the Topology Discovery phase at the originator.
2. Packets are forwarded by enhancing the Ad-hoc routing protocols such as DSR and AODV depending upon the attack identified.

## VI SIMULATION AND EPERIMENTAL RESULTS

The physical layer of a wireless network is often vulnerable to denial of service attacks such as jamming. Mechanisms such as spread spectrum have been extensively studied as means of providing resistance to physical jamming, and we thus disregard such physical layer attacks here. We assume that network links are bidirectional; that is, if a node A is able to receive packets transmitted directly by some node B, then B is able to receive packets transmitted directly by A. To decline link failure symmetric communication is enabled. It is possible to use a network with unidirectional links if such links are detected and avoided; such detection may also otherwise be necessary, since many wireless Medium Access Control protocols require bidirectional links, as they make use of bidirectional exchange of several linklayer frames between a source and destination to help avoid collisions and improve reliability.

Result analysis is done by the network assumptions with every mobile node moving based on mobility data files that were generated by mobility generator module. The transmission range is fixed at 250 units. The number of nodes varies from 50 to 100. The Node 0 is initialized to be the server node by default. A cache node is maintained for every 5 client nodes created. The nodes transfer data through routing protocols as discussed throughout the network. Maximum speed of node is set to 10 m/sec. All nodes do not stop moving until the simulation time 500 seconds is reached.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

The evaluation statistics shows that when less number of nodes have in connection through mobility the time delay is reduced apparently. Whereas, the IDS mechanism corresponding to the packet delivery ratio at 5:1 proves effective outcome.

| **Scenario Parameters** | |
|---|---|
| Number of nodes | 50 |
| Maximum velocity ($V_{max}$) | 20 m/s |
| Dimension of space | 1500m * 300m |
| Nominal radio range | 250m |
| Source-Destination pairs | 20 |
| Source date pattern (each) | 4 packets/second |
| Application data payload size | 512 bytes/packet |
| Total application data load | 327 kbps |
| Raw physical link bandwidth | 2 Mbps |
| **Routing Protocol parameters** | |
| Initial RREQ timeout | 2 seconds |
| Maximum RREQ timeout | 40 seconds |
| Cache size | 15 routes |
| Cache replacement policy | FIFO |

Table 1 Simulation parameters

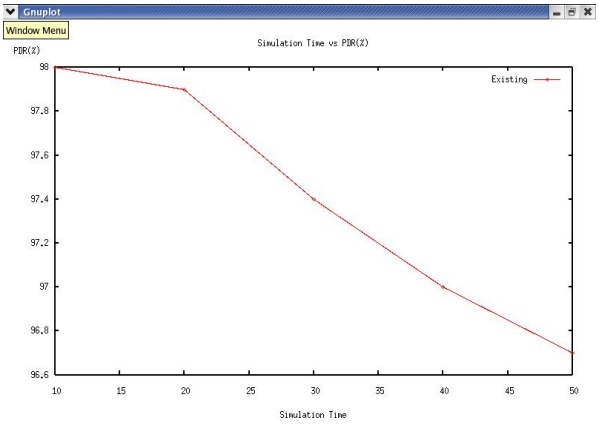


Fig. 7 Simulation Time Vs. Packet Delivery Ratio

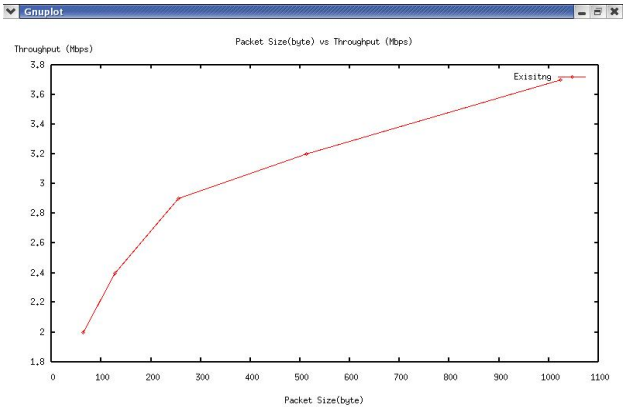


Fig. 8 Packet size Vs. Throughput

## VI. CONCLUSION AND FUTURE WORK

In Ad-hoc wireless networks transmitting packet from source to destination through dynamic topology is analyzed with two considerations: (i) It maintains legitimate nodes during packet forwarding such that routing is performed in an optimal path and effective handling of nodes when attacker is involved (ii) Secondly, even in the presence of an attacker the packet is sent to destination with at most minimum draining battery power by maintaining HN certification and cache consistency mechanism the nearest neighbor to the destination is easily identified.

Two types of attacks were discussed: They are Stretch attack and Carousel attack. Both attacks results in draining of battery power by estimating a non-optimal path by the attacker. In such cases, the packets are forwarded by tracing the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 2, Issue 4, April 2014**

PLGPa protocol with no- backtracking property. So the DSR routing protocol here used selects the best from the multi-path routing estimates at the time of link failure, such that resilient forwarding is achieved. When both attacks are encountered simultaneously then Stretched Cycle attack is possible. This is handled by the proposed D-PLGPa (DSR extended with PLGPa) routing protocol when a node receives same packet more than once. The possibility of both the attacks together, Streched Cycle attack can be handled by increasing the existence of the proposed system description In the future enhancement, attacks such as blackhole attack and malicious discovery attack can be handled by extending the Detection mechanisms effectively with the routing protocol to reduce draining power by discovering an optimal path. In such cases, a performance evaluation with consideration of more number of nodes can be analyzed.

## REFERENCES

1. Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, "Secure sensor network routing: A clean-slate approach", CoNEXT, pp 2-10, 2006.
2. Kihong Park and Heejo Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack" , INFOCOM, pp 4-8, 2001.
3. Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks", IEEE transactions on mobile computing vol.12 no.2, pp 1-12, 2013
4. Mingze Zhang, Mun Choon Chan and A. L. Ananda, "Location-Aided Topology Discovery for Wireless Sensor Networks" , IEEE Conference on Communications, pp 2718-2722, 2008
5. Wayne Jansen, Peter Mell, Tom Karygiannis and Don Marks, "Applying Mobile Agents to Intrusion Detection and Response" , U.S Department of commerce Technology Administration, pp 18-24, October 1999
6. Yih-Chunhu and Adrian Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad HocNetworks" , Wireless networks 11, 2138 Springer, pp 25-30,2005
7. Liangzhong Yin and Guohong Cao, "Supporting Cooperative Caching in Ad Hoc Networks" , National Science Foundation CAREER CCR009227 and ITR-0219711, pp 4-10, 2005
8. Po-Wayau, Shenglan Hu and Chris J. Mitchell, "Malicious attacks on ad hoc network routing protocols", Information Secutiry Group, Royal Holloway, University of London, pp 230-260, 2006

## BIOGRAPHY

**Preethi Monolin.P** is a Post Graduate student in the Masters of Engineering in Computer Science Department, Alpha College of Engineering, Chennai, Tamil Nadu, India. She received Bachelors of Engineering in Computer Science Department in 2012 from Kings Engineering college, Chenaai, Tamil Nadu, India. Her research interests are mobile computing, creative web designing, and computer networks.