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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

LAL Methodology to Mitigate Denial of Service Attacks in Fictitious Nodes Used in OLSR Protocol

Aditya Kathera[1], Adithya. R[2] , G. Gokulnath[3], Tarun Raj Moturu[4]

Student, Department of Computer Science and Engineering, SRM University, Ramapuram, Chennai, India[1]

Student, Department of Computer Science and Engineering, SRM University, Ramapuram, Chennai, India[2]

Student, Department of Computer Science and Engineering, SRM University, Ramapuram, Chennai, India[3]

Student, Department of Computer Science and Engineering, SRM University, Ramapuram, Chennai, India[4]

ABSTRACT:Mobile ad-hoc network is designed to operate effectively over farther distances. This technology follows store-carry-forward mechanism using bundle protocol to make data forwarding without any discontinuations. However due to security vulnerability, the network faces serious threat such as black hole attack and malicious behaviour. These defective nodes may delay the network performance and consume a lot of network resources; as a result, they constitute an important problem that should be well thought-out. The purpose of this paper is to identify defective nodes using LAL methodology.

KEYWORDS: OLSR Protocol; LAL; Denial of Service (DOS) attack; Greedy Perimeter Stateless Routing Protocol (GPSR); Greedy Forwarding; Network Simulation (NS2); OTcl; Xgraph

I. Introduction

A group of mobile devices that are capable of wirelessly communicating with one another without any use of centralized authority or pre-determined infrastructure can be defined as a Mobile Ad Hoc Network (MANET) [15]. The battery power of nodes in MANET is very constrained and is very limited, they cannot be replaced or recharged in intricate situations. The consumption of energy for each node is dependent on its communication state: transmitting, listening or sleeping mode. There could be large chances of packet and information loss in between nodes while communication which can in turn be referred to denial of service attack (DOS).

In this paper we recognise the DOS attack in the fictitious nodes and present a method in order to mitigate it. Our solution, Localizability aided localization provides a method to prevent DOS attack by creating a centralised node and processing the communication. Moreover, LAL utilises the techniques used in DCFM method and further provides a clear solution in order to avoid DOS attack in them. Through empirical data, we demonstrate that (1). The technique proposed avoids the majority of DOS attacks (2). Lastly, this methodology can also be utilized in similar DOS attacks in OLSR.

The content of this paper is organized as follows. In the second section the OLSR protocol, denial contradiction with fictitious node and localizability aided localization method have been accordingly discussed. The methods to avoid denial of service attacks in fictitious nodes is described clearly in Section 3. Section 4 represents the simulation module and the outputs achieved. Finally, the conclusion with future works are represented in Section 5.

II. MODULE DESCRIPTION

Optimized Link State Routing Protocol:

An Optimized Link State Routing Protocol (OLSR) is said to be a proactive, link state routing protocol. The algorithm which is under link state routing protocol chooses the finest route by determining a range of characteristics like delay, link load, bandwidth etc. The calculation of the finest route and additional complicated than hop count, which is said to be under link state routes in OLSR which is more stable, reliable and accurate. For updating the topological info rations in each node, the broadcasting of message is periodic over the network. Multipoint relays are used to facilitate efficient flooding of the control message in the network. The calculations of the route are done by multipoint relays which lead to the formation of the route from a specified node to any destination in the network. The development of OLSR protocol is to work separately from other protocols. Theoretically, there are three generic elements in OLSR: neighbour sensing mechanism, efficient flooding of control traffic mechanism, and a requirement of how to select and diffuse adequate topological information in the network in order to prove optimal routes. The requirement of message types for the mainstay functionality of OLSR are: HELLO-messages, link sensing task performance, neighbour detection and MPR signalling, TC-messages, topology declaration task performance, MID-messages, declaring the presence of multiple interfaces on a node task performance.

Denial contradiction with Fictitious Node:

The method of HELLO message does not verify actively, relatively it checks the integrity by searching for the contradiction between the HELLO message and the identified topology.

- Relays under Multiple points

The control messages flooding in the network is been minimized under multi point relay.

- Network Formation

To create multiple nodes by giving distance and range and based on coverage the neighbour node will be detected.

- MPR Nodes Recognition

By clicking the fictitious node button by single hop neighbours to choose which has to be elected as MPR.

- Attack of Node Isolation

The particular node called as the fictitious node performs the attack which leads to separation of the opposite node totally from the whole network. By the decrease of the TC Message from the target node, the separation of the opposite node is done.

- Detection of the Attack and System Recovery

The destination node of exact waiting time is called as the timeout period in which it has to collect the data packet and weakening the attack which has been suspected in the network. It as well informs all other nodes about the fake MPR and the OLSR table which contain the MPR List of all the nodes within the network has to be updated automatically. After the MPR update, the sending of a data packet through the right MPR which arrives at the destination.

Localizability Aided Localization Method:

Localizability Aided Localization (LAL) consists of three different phases: structure analysis, node localizability testing and network adjustment. LAL activatesa single round adjustment, which further carries out few popular localization methods.

III. Proposed System

A.*Node Localizability Testing:*

The limitation of node localizability has been analysed by the earlier mechanism and proposition of novel concept. By deriving the conditions which are necessary and sufficient for node localizability for the first time, it is possible to locate the node in even sparsely or moderately connected networks by analysing several nodes.To authorize the design, the execution is done with the solution by showing the node localizability which provides a useful procedure for network deployment and other location- based services for a real-world system and the experimental results. In recent years, several approaches have been projected for in-network localization, in which the global location is known by some special nodes (called beacons or seeds) and the rest of the locations have been determined by measuring the Euclidean distances to their neighbours. The initial major challenge to recognize uniquely localizable nodes has been made by studying node localizability. The subsequent network localizability results and to locate a localizable sub graph from the distance graph by identifying all the nodes in the sub graph localizable is said to be an obvious solution. Unfortunately, the attempts which are forthright miss a few viably localizable nodes and mistakenly identify them as non-localizable nodes. On deriving the necessary and sufficient conditions for node localizability, the answer to the fundamental questions on localization can be obtained.These designs not only surpass the previous ones theoretically, while they also achieve a decent performance for practical uses.

B. *Structure Analysis:*

The study of extensive social sciences has been done on networks. The circulation of questionnaires involves in sociology are under the study of typical networks, detailed interaction with others is done by asking respondents. The responses are used by one of them in which vertices symbolize individuals and edge the interactions between them by the reconstruction of networks. The study of address issues of centrality and is made by the typical social network. Initially, to understand the meaning of these properties with the help of creation of model networks—how they came to be as they are, and how the interaction process is done with one another. Third, the prediction is made with the behaviour of networked systems which is entirely based on measured structural properties and the governing of local rules by individual vertices. How will the structure of the network affect traffic on the Internet, or the dynamics of social or biological systems, or the Web search engine performance? As we see, the scientific community has a broad variety of disciplines by drawing on ideas and made an excellent start on the characterization and modelling of network structure.

C.*Network Adjustment:*

As the proliferation of wireless and mobile devices continues, a wide range of context-aware applicationsare deployed, including smart space, modern logistics and so on. In these applications, location information is the basis of other services, such as geographic routing, boundary detection, and network coverage control. In some other applications, such as military surveillance and environment monitoring, sensed data without location information are almost useless. The primary problem in wireless ad hoc and sensor networks is that each individual node determines its own location. In this work, we focus on 2D in- network localization -in which some special nodes (called beacons or anchors) know their individual global locations and the rest of the nodes determine their Euclidean coordinates by measuring the Euclidean distances from or between their neighbours. Due to deployment or hardware restrictions, a network can be partly localizable given the distance and locations of all the beacons, specifically, some nodes have unique locations while others do not as distance is only a scalar parameter. To identifynodes that do not have any unique location, the availablesolutions mainly focus on the tuning of network settings. Deploying additional nodes or beacons in the application fields is the first attempt. The localizability can be enhanced by increasing node density which occurs due to increased deployment and abundant internode distance constraints.Yet, this attempt lacks viability, as the additional nodes need to be placed in the vicinity of non-localizable nodes, whose locations are undetermined. Using mobile nodes like beacons is another option. The controlled motion of beacons provides detailed information for localization, but also acquirescontrolling overheads and adjustment delay.

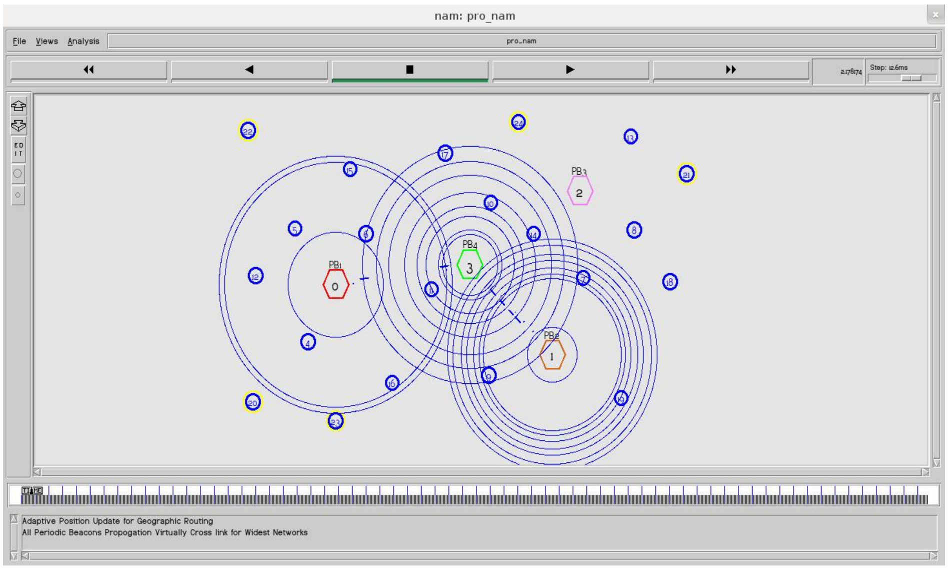
D. *Greedy Perimeter Stateless Routing Protocol (GPSR):*

Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks has been used to make packet forwarding decisions by using the positions of routers and packet’s destination. GPSR, is a liable and effective routing protocol for mobile and wireless networks. Greedy forwardingdecisions are made with the available information about the router’s neighbours in the network topology and thus forwards packets to the nodes that are closer towards the destination.The algorithm recovers by routing around the perimeter of the region in some cases where greedy forwarding is not possible.While considering local topology, as the number of network destinations increases, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols. The Distance Vector (DV), Link State (LS), and Path Vector routing algorithms have been well established as the topology changes more rapidly on a mobile, wireless network than on wired networks. Rate of change of topology and the number of routers in the routing domain are the primary factors that determine the scaling of a routing algorithm. These factors affect the message complexity of DV and LS routing algorithms.

E. *Greedy Forwarding:*

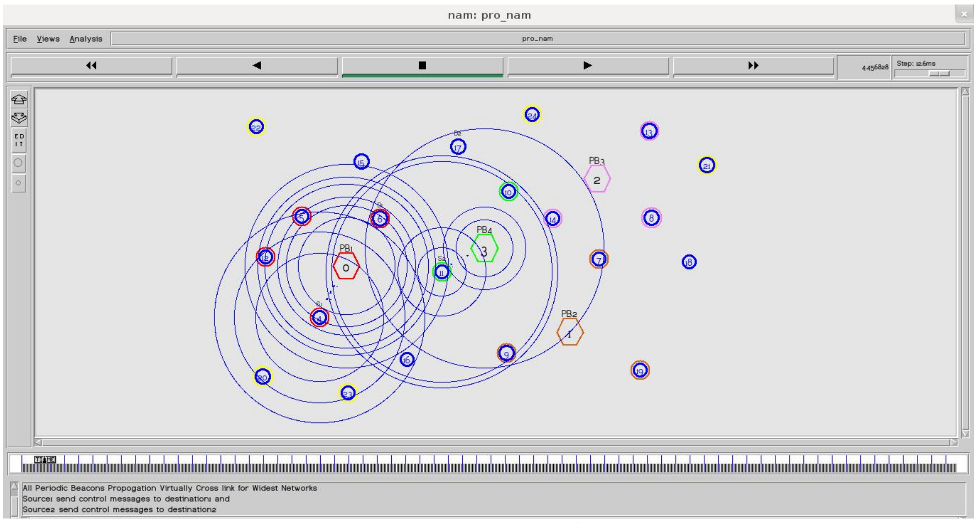
Under GPSR, packets are marked by their originator with their destinations’ locations. Consequently, the forwarding node can make an ideal choice while selecting the packet’s next hop. If a node can identify its radio neighbour’s positions, the ideal choice of next hop is the neighbour, geographically closest to the packet’s destination. We putrefy a distance graph into two-connected components that support fine-grained manipulation. These components are additionally organized in a tree structure and, the one consisting beacons is the root and adjustments are conducted along the tree edges from the roots to leaves of the tree structure. LAL converts all the non-localizable nodes in one round via the method of vertex augmentation. Therefore, we take up a location registration and lookup service that maps the node addresses to their locations.

IV. SIMULATION RESULTS



Adaptive Position Update for Geographic Routing
All Periodic Beacons Propogation Virtually Cross link for Widest Networks

Fig. 1. Cross link optimization for large network



All Periodic Beacons Propogation Virtually Cross link for Widest Networks
Source1 send control messages to destination1 and
Source2 send control messages to destination2

Fig. 2. Data transmission using authentication

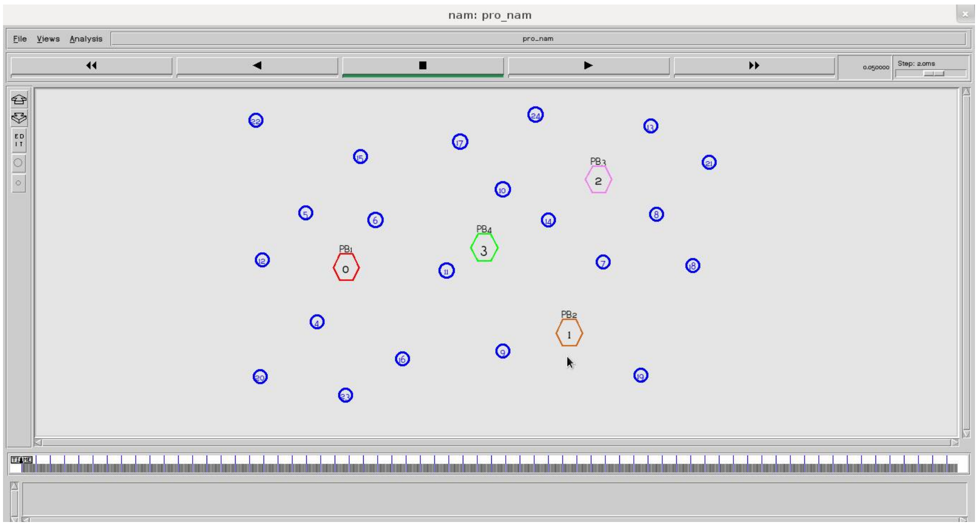


Fig. 3. Network formation

NETWORK SIMULATION 2:

NS (Version 2) is an object oriented, discrete event driven simulator coded in languages, C++ and OTcl is an open source network simulation tool. It. The network protocols such as TCP and UPD, traffic source behaviour such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and many more can be implemented with the help of NS.

NS2 separates the control and data path implementations. The simulator supports two different hierarchies, a class hierarchy in C++ known as the compiled hierarchy and a corresponding hierarchy within the OTcl interpreter called interpreted hierarchy.

NS2 primarily uses two different languages because it is necessary to increase the runtime speed and simulation of protocols requires efficient manipulation of bytes. Conversely, in network studies the primary goal is to change some parameters and to scrutinize a number of scenarios, the time to change the model and to run it again is highly important.

In NS2, the protocol implementation is done by using C++ and in general for such cases where every packet of a flow has to be processed. For instance, if you want a new queuing discipline to be implemented, then C++ is the preferred programming language. OTcl, alternatively, is suitable for configuration and setup, although the runtime of OTcl is slow,can be changed instantly and the construction of simulations can be made easier. In NS2, the OTcl interpreter can access the compiled C++ objects. Therefore, the OTcl level can control the readymade C++ objects.

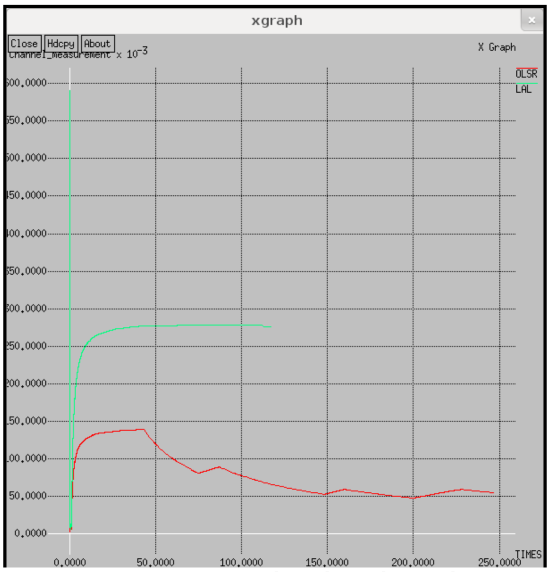


Fig.1. Channel signal strength

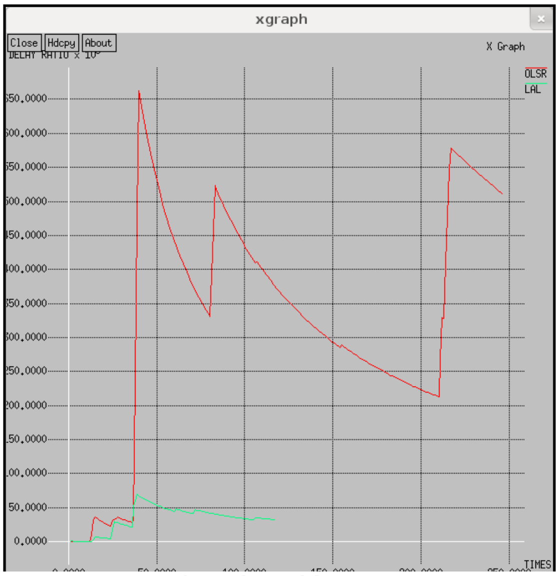


Fig. 2. End to end time delay

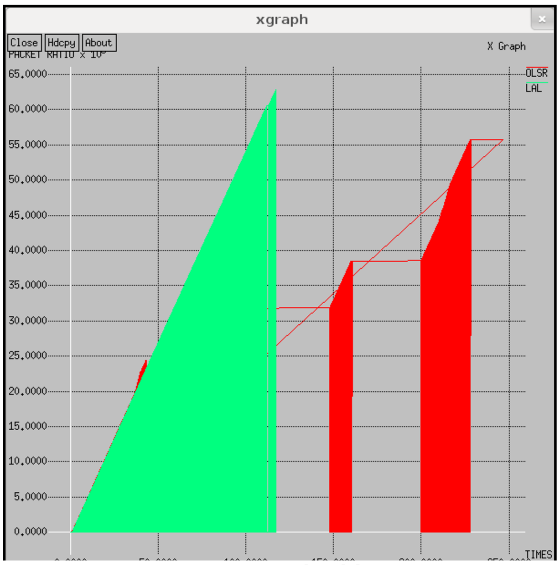


Fig. 3. Packet delivery ratio

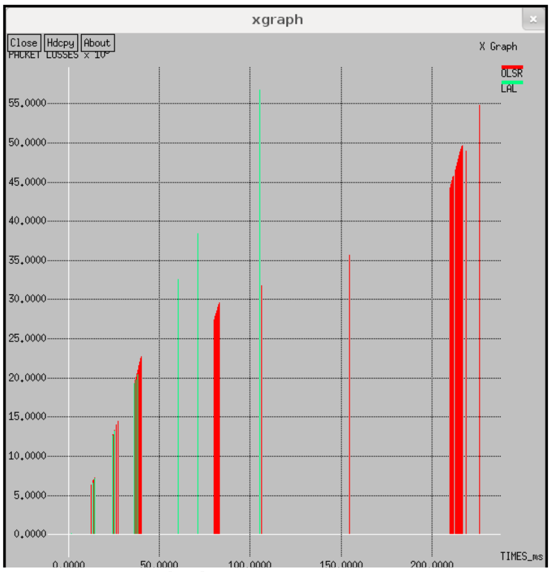


Fig 4. Packet loss ratio DOS

V. CONCLUSION AND FUTURE WORK

The proposed Localizability Aided Localization algorithm will provide the solutions to packet loss and data rate tradeoff against the Denial of Service attack in a given network. The foremost contributions of this study are as follows:

- Considering node localizability, the adjustments done by LAL are selected which in turn avoids hollow ranging and communication costs.
- LAL works fine with the existing localization methods without any subjects of incompatibility.
- Lastly, we implement LAL on a real sensor network consisting of nodes. The data is collected from empirical situation in large application field. However due to security vulnerability, the network faces serious threat such as black hole attack and malicious behavior. These Misbehaving nodes may delay network performance and consume network resources, therefore constituting an important problem that needs to be considered and resolved.

Future Scope:

- Our Future work focuses on detecting misbehaving nodes using RSA. The RSA algorithm is a public key cryptographic algorithm. The RSA keys should be generated if none are found. The key generation process is often slow but is barely performed. The following steps are involved:
    1. Key Generation, Encryption and Decryption :

Encryption: When the source wants to send message M to destination The Destination node transmits its public key (n, ,e) to Source node and keeps the private key secret then source wants to send message M to Destination It first turns M into an integer 0 <m <n by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c corresponding to:c=memodn.

Decryption: Destination node can recover m from c by using its private key exponent d by the following computation: Given m, Destination can recover the original message M by reversing the padding scheme. m=cdmode.

REFERENCES

1. GautamBarua,Manish Agarwal, 'Caching of Routes in Ad hoc On-Demand Distance Vector Routing for Mobile Ad hoc Networks'.
2. Mahmood Salehi, HamedSamavati,'Injection and Evaluation of New Attacks on Ad hoc Proactive Routing Algorithms', International Journal for Information Security Research (IJISR), Volume 2, Issues 1/2, March/June 2012.
3. Prof.Masrath Begum,Nitesh.S.P, 'Secure MANET'S from DOS Attack using EOLSR', International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 7, July 2014.
4. K.P. Manikandan,Dr.R.Satyaprasad,Dr.K.Rajasekhararao, 'A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks', (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.
5. R.Arunkumar, Mrs. A.Annalakshmi,'A Recent Analysis of Intrusion Detection and Prevention System for Protecting Range of Attack using Data Gathering Technique in MANET', International Journal of Computer Applications (0975 – 8887),Volume 85 – No 8, January 2014.
6. C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994.
7. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Proc. IEEE Int. Multi Topic Conf. Technol., 2001.
8. T. Clausen and P. Jacquet, "RFC 3626-Optimized Link State Routing Protocol (OLSR)", 2003.
9. C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the olsr protocol," in Proc. Med-Hoc-Net, 2003.
10. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Commun., vol. 14, no. 5, Oct. 2007.
11. D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," Dynamic Source Routing Protocol (DSR) Mobile Ad Hoc Netw. IPV4, 2007.
12. D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an ids to safeguard olsr integrity in manets," in Proc. Int. Conf. Wireless Commun. Mobile Comput., 2006.
13. D. Raffo, C. Adjih, T. Clausen, and P. M€uhlethaler, "An advanced signature system for OLSR," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004.
14. A. Adnane, C. Bidan, and R. T. de Sousa Junior, "Trust-based security for the olsr routing protocol," Comput. Commun., vol. 36, no. 10,2013.
15. S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777. [Online]. Available: http://www.google.com/patents/US20060176829

BIOGRAPHY

Aditya Katherais a final year student in the Computer Science Department, SRM University, Ramapuram. He has received Certified Ethical Hacking (CEH) certification by EC council in the year 2015. His research interests are Artificial Intelligence, Human Computer Interaction, Web application attacks and others.

Adithya.R is a final year Computer Science student at SRM University, Ramapuram. His research interests include Artificial Intelligence, Wireless Networks, and Wireless Sensor Systems.

Gokulnath is a final year Computer Science student at SRM University, Ramapuram. His research interests include Artificial Intelligence, Computer Graphics, and Computer networks.

Tarun Raj Moturu is a final year Computer Science student at SRM University, Ramapuram. His research interests include Artificial Intelligence, Cloud Computing, and Computer Security.