

North Asian International Research Journal Consortium

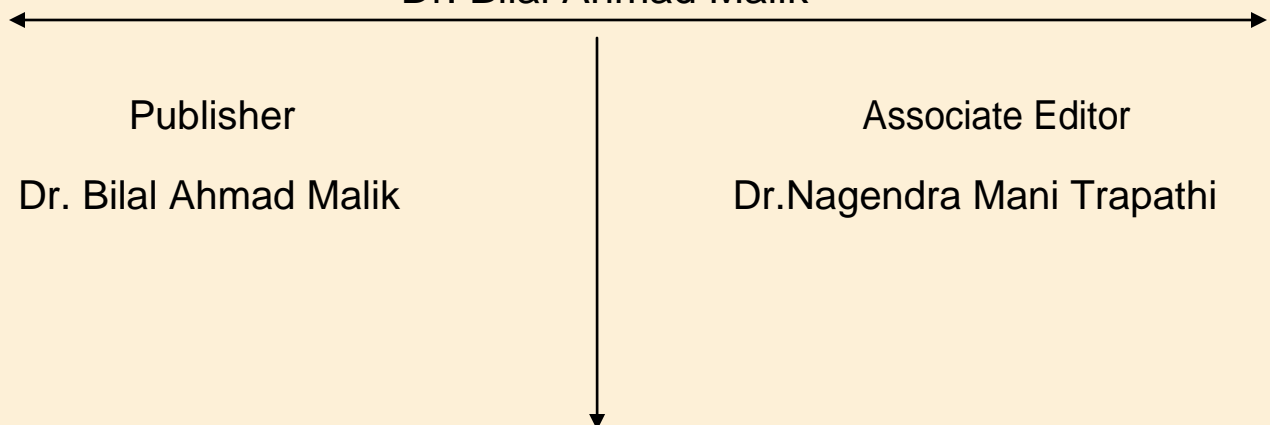
North Asian International Research Journal

Of

Science, Engineering and Information Technology

Chief Editor

Dr. Bilal Ahmad Malik



NAIRJC JOURNAL PUBLICATION

North Asian
International
Research Journal Consortium



Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

M.C.P. Singh Head Information Technology Dr C.V. Rama University	S.P. Singh Department of Botany B.H.U. Varanasi.	A. K. M. Abdul Hakim Dept. of Materials and Metallurgical Engineering, BUET, Dhaka
Abdullah Khan Department of Chemical Engineering & Technology University of the Punjab	Vinay Kumar Department of Physics Shri Mata Vaishno Devi University Jammu	Rajpal Choudhary Dept. Govt. Engg. College Bikaner Rajasthan
Zia ur Rehman Department of Pharmacy PCTE Institute of Pharmacy Ludhiana, Punjab	Rani Devi Department of Physics University of Jammu	Moinuddin Khan Dept. of Botany Singhaniya University Rajasthan.
Manish Mishra Dept. of Engg, United College Ald.UPTU Lucknow	Ishfaq Hussain Dept. of Computer Science IUST, Kashmir	Ravi Kumar Pandey Director, H.I.M.T, Allahabad
Tihar Pandit Dept. of Environmental Science, University of Kashmir.	Abd El-Aleem Saad Soliman Desoky Dept of Plant Protection, Faculty of Agriculture, Sohag University, Egypt	M.N. Singh Director School of Science UPRTOU Allahabad
Mushtaq Ahmad Dept.of Mathematics Central University of Kashmir	Nisar Hussain Dept. of Medicine A.I. Medical College (U.P) Kanpur University	M.Abdur Razzak Dept. of Electrical & Electronic Engg. I.U Bangladesh

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

SECURE PROACTIVE SOURCE ROUTING FOR WIRELESS NETWORKS

M.HIMA BINDU*

*M.Tech (Computer Science), Department of CSE, JNTUA College of Engineering, Anantapuramu, A.P, India.

S.VASUNDRA**

**Professor, Department of CSE, JNTUA College of Engineering, Anantapuramu, A.P, India.

ABSTRACT:

Mobile ad hoc network (MANET) is a self-configuring wireless communication network without any pre-existent infrastructure. A network is formed by the nodes whenever they want to communicate and leave the network when there is no need of it by using opportunistic routing. Due to this, topology changes dynamically. With this an intruder can easily enter into the network as a trustee node and drop the packets from reaching the destination. Packet dropping leads to DOS (Denial of Service) attack. By, using an Intrusion detection system (IDS) can overcome packet dropping. It monitors the forwarded packets and detects a malignant node that causing an intrusion. When it finds an intruder in the specified route, redirects the packet in another path and to prevent it from losing the information.

Keywords: MANET, opportunistic routing, IDS

I. INTRODUCTION:

Mobile ad hoc network (MANET) is a multi-hop wireless network without an existing infrastructure. It establishes a transient network whenever it needs to communicate. Nodes dynamically establish routing among themselves to move arbitrarily. It configures the network on its own i.e., where the nodes itself act as a router. The challenges are loss of packet with the presence of interference, frequent path breaks; security violation due to its dynamic topology. Bluetooth and Personal area network, military battlefield [1], commercial sector and collaborative work are some of the applications of the MANET.

In MANET, the network connectivity is intermittent and topology changes dynamically. To tolerate against these issues, Opportunistic routing [8] provides a promising solution. Data forwarding and routing plays a major role at the network layer. Forwarding the data with appropriate nodes through a specific route can minimize overhead and increase the throughput. Based on the opportunity, a group of forwarding nodes cooperatively selects a node that made a path close to destination. There are many routing protocols that take a different routing strategy.

Proactive source routing (PSR) [9] is a lightweight protocol that facilitates opportunistic routing. The entire network in the form of spanning tree rooted at each node. To get the updated network topology the information among them is exchanged with the adjacent nodes. With this, each node has complete knowledge about the topology and if any changes occur they can be easily identified. In next iteration these changes get updated and can decrease the delay in routing. Because of its ad hoc nature, an intruder can occupy a place in network and changes the behaviour of the node as a malign to perform an active attack.

In this paper, to forbid these attacks the proactive source routing (PSR) with an (IDS) [7] intrusion detection technique is employed. It detects an intruder by monitoring network traffic and prevents from data lose and analyses a whole network for envious activities [10] and forwards this information to get rid of attack.

The rest of the paper is organised as: Section II specifies the work related to the different protocols and security measures. Proposed work is described in section III and section IV describes the future scope with the conclusion.

II. RELATED WORK:

By choosing applicable routing protocols can minimise the overhead by the bulk of unused information stored at each node. In MANET the protocols categorised as [5] proactive and reactive. Proactive routing is also named as table-driven, it is so called because that every node maintains a table with the information about the neighbouring nodes. DSDV [3] and OLSR are the examples of table-driven routing. Reactive routing is also called as on demand routing. The source initiates the path when it needs to send the data. DSR [4] and AODV [6] are examples of on demand routing.

DSDV (Destination sequenced distance vector) is an extension to DV (Distance Vector) algorithm. In DV each node has a distance cost associated with it. Based on the information received from neighbours it chooses the path with the least cost that gives an optimised route. It suffers from count to infinity problem. DSDV provides a solution by adding a sequence number after each broadcast.

DSR (dynamic source routing) is a reactive, when a node wants to send data at that time it go for a route search without any prior information. Once path is identified in return search entire path embedded in each node data packet up to the receiver. Here the path is initiated by the source node and all of the remaining nodes travel along this path. Once the link gets retired, the data will be lost because it doesn't have any predefined information about it.

DSDV, AODV (Ad-hoc On Demand Distance Vector) are not opted for source routing. Hence they do not provide an opportunistic routing. Even though OLSR [2] (Optimised Link State Routing) and LS(Link State) algorithms are of table- driven , are suitable for source routing; LS having an idea about whole network choose a path on its own. But it consumes high battery power due to every node floods an information about the links to itself and adjacent nodes which leads to duplications and overhead. With MPR (Multi Point Relay) in OLSR an extension to LS avoids unnecessary transmissions but not the overhead.

Hence by using lightweight PSR (Proactive Source Routing) that maximises the throughput with less overhead at maximised bandwidth. PSR initiates a source routing with a prior knowledge about the network by BFS (Breadth First Search) tree rooted at each node and thus providing an opportunistic routing. It is a tree based routing where updates can easily integrate into the topology. It broadcasts the packet in a binary representation format. If it has a neighbouring node either on its left or right is indicated by 1 otherwise by 0. By this size of a message can be minimised. While any changes or node lost it tries to keep the stable topology without changing the overall tree by minute changes. By implementing all these PSR employs a less fraction of overhead.

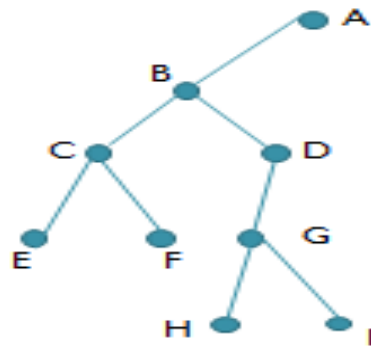


Fig 1: Breadth First Search Tree

Apart from routing, security is the most important factor to be considered. By using encryption techniques provide security against outside attacks. The inside attacks by the nodes of the network can be found by intrusion detection system [11].

III. PROPOSED WORK:

Proactive source routing (PSR) provides a secure routing with intrusion detection technique (IDS). It is used to provide security by personnel aware of packets with the monitored network. An IDS performs the detection in multiple ways. In Misuse-based detection, a pattern compares a susceptible threat with the attack class previously stored in the IDS. Another type is an anomaly- based detection technique by using this IDS looks for vulnerabilities based on rules set forth by user i.e., compare the normal event against characteristics making the event as abnormal.

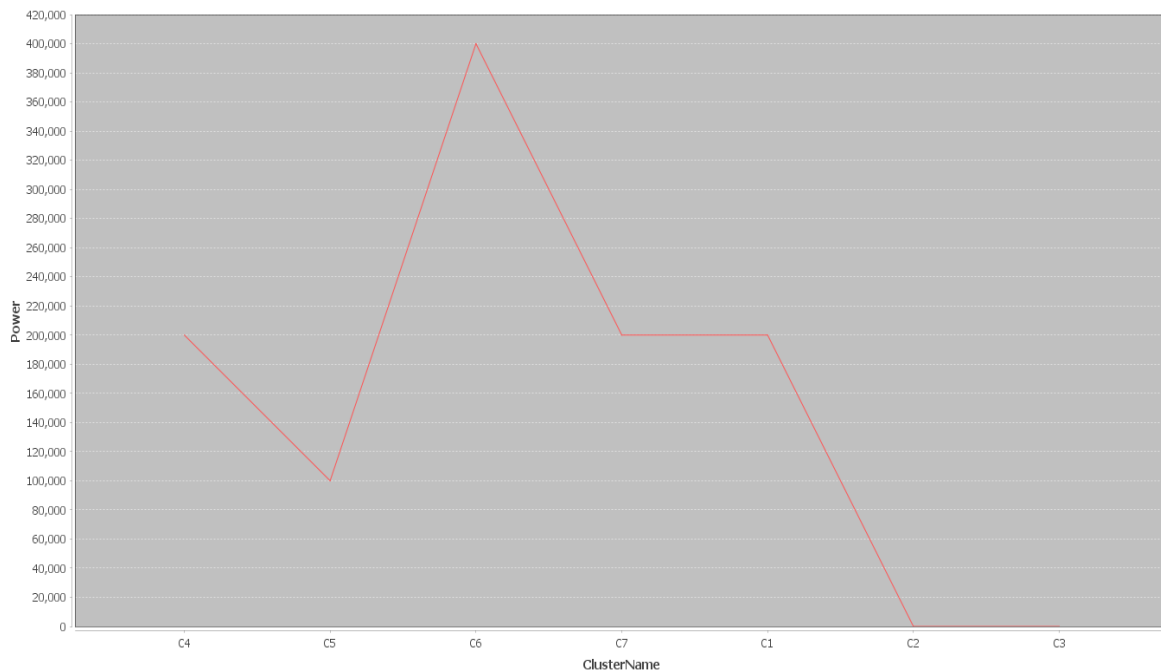
With the limited battery power in MANET, to place IDS at each node is not possible i.e., each node in the network as a monitoring node. Instead the neighbouring nodes that are close with one other made into a cluster. PSR is a tree structured routing; the nodes that require an intermediary form into one cluster. Select a node in the cluster as a head to make it as the monitoring node with IDS. By averaging all the weights associated with every node and then select the one i.e., less than average or randomly elect a node as head. The node elected as clustered head analyses and monitors the traffic for intruders those cause attacks. It has the information about all other nodes within that cluster. Share the information with the neighbouring clusters.

Each node randomly generates a value. With the least value it chooses the path that makes the optimised route with less overhead. Even though an intruder occupies a node in the network and attacks in the route that is followed by a packet .IDS prevents it from dropping the packet. When an intruder attacks a node the attack details are captured by an IDS .While sending data to destination node IDS manager checks the status of each node to verify whether any node is attacked or not. If so, it redirects the packet through another route that gives high throughput without losing the data.

Rule- based matching use the features to identify intrusions. It is knowledge based equipped with database having node energy and compares the collected data with the content database. Initially it multicast the packet to detect an intruder as IDS has a database about all nodes and any changes in the node energy specifies an attack on that node. When a provider sends a file to receiver it calculates time and energy of a node. The intruder attacks the node by making its energy to zero.

If the node energy is normal as before the packet has multicast then it means no intruder is there otherwise an IDS manager alerts the network by declaring a node attacked by an intruder that mark the node energy to an abnormal state by assigning it to zero. An IDS updates the database with the intruder details i.e., which node gets intruded and multicast this information about an intruder to all of its neighbours. Therefore, all nodes update their database about malicious node along with other nodes. Even if an intruder attacks it can easily identified and for getting a normal state of node from an abnormal state, by modifying the power of a node. If a node is in abnormal state, it gets easily attacked by an intruder. With opportunistic routing the nodes that are not listed as intermediaries by source routing can also be used as interims because an IDS has full idea about all nodes and perform a secure routing with these nodes also.

Here, the Anomaly detection technique identifies the anomalies that change the node state from normal to abnormal position. The node power is considered as an anomaly because an intruder deviate the node energy from its initial position to idle. However, with IDS the packets can route in a secured manner without any implications. Selfish nodes that cause the insider attacks affect the throughput of network and this can be reduced by detecting those nodes. Finally a database with the information about the malignant nodes and other remaining nodes is maintained by IDS. With this data the packets can send without leading to an attack and in a protected way.

RESULT:**Fig 2: Detection of an intruder**

By using JFreechart plot the graph. It represents the node that gets attacked by an intruder in a specified cluster. Here it specifies the node attacked by an intruder in the cluster c2 and c3.

IV. CONCLUSION & FUTURE WORK:

MANET is a communication network that establishes an ad-hoc network. The network that changes dynamically consumes a lot of battery and an intruder can easily enter into a network and attack the node. The first issue can be minimised by opportunistic data forwarding. It is facilitated by proactive source routing (PSR) with less overhead and maximising the throughput. Another issue of an intruder can be solved by providing IDS. It detects an intruder and if the packet forwarded by a malignant node i.e., attacked by an intruder it redirects the packet through another route that is nearer to the destination otherwise it follows the same route.

It detects an intruder but doesn't specify the attack type it is particularly i.e., whether an impersonation attack or black hole attack etc., The future work can deal with this issue.

REFERENCES:

- [1]. Mr.Kaushal Kishor, Dr. Parma Nand, “Review Performance Analysis and Challenges Wireless MANET Routing Protocols,” International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 10, October 2013
- [2] Vivek Sharma and Bashir Alam, “Unicast Routing Protocols in Mobile Ad Hoc Networks: A Survey”, International Journal of Computer Applications (0975 – 8887), Vol. 51, No.14, August 2012.
- [3] B.N. Jagdale, Pragati Patil , P. Lahane , D. Javale , “Analysis and Comparison of Distance Vector, DSDV and AODV Protocol of MANET ,” International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012
- [4] Rajesh Sharma, Seema Sabharwal, “Dynamic Source Routing Protocol ,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013
- [5] Shaheen Khan, Dr. Javed Khan Bhutto, Gautam Pandit, “Reactive and Proactive Routing Protocol Performance Evaluation for Quantitative Analysis in MANET,” International Journal Of Scientific Research And Education Volume 2, Issue 12, Pages-2540-2551 December-2014 , ISSN (e): 2321-7545.
- [6] Humaira Nishat , Vamsi Krishna K , Dr. D.Srinivasa Rao and Shakeel Ahmed, “Performance Evaluation of On Demand Routing Protocols AODV and Modified AODV (R-AODV) in MANETS,” International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.1, January 2011
- [7] S. Umang¹ B.V.R. Reddy¹ M.N. Hoda², “Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption”, IET Communication Vol. 4, Iss. 17, pp. 2084–2094 - 2010.
- [8] Z. Wang, Y. Chen, and C. Li, “A New Loop-Free Proactive Source Routing Scheme for Opportunistic Data Forwarding in Wireless Networks,” IEEE Communications Letters, to appear.
- [9] Z. Wang, Y. Cheng, and C. Li, “PSR: A Lightweight proactive source routing protocol,” IEEE Trans. Veh. Technol., vol. 63, no.2, pp. 859- 868, Feb. 2014.
- [10] Haripriya ,Y,Pavani KVB, Lavanya S, Viswanatham VM . “ A framework for detecting malicious nodes in mobile Adhoc network ,”Indian Journal of Science and Technology.2015 Jan; 8(S2):151-5.
- [11] Dr.S.Vasundra, S.MothiVenkata Manoj, “An efficient protocol for secure communication in Wireless Ad Hoc Networks ,” International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2014

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper, Summary of Research Project, Theses, Books and Book Review for publication.

**Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301**

Jammu & Kashmir, India

Cell: 09086405302, 09906662570,

Ph No: 01933212815

Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com

Website: www.nairjc.com

