International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 3, June 2017, pp. 1197~1203
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i3.pp1197-1203

Node Disjoint Random and Optimal Path Selection (NDROPS) Algorithm for Security in MANETS

P. Suma[1], O. Nagaraju[2], Md. Ali Hussai[3]
[1]KL University, Guntur, India
[2]Department of CS, Government College, Macherla, Guntur, India
[3]Dept. of Electronics and Computer Science Engineering, KL University, Guntur, AP, India

Article Info

Article history:

Received Dec 9, 2016
Revised May 9, 2017
Accepted May 23, 2017

Keyword:

Attacks
MANETs
Node-disjoint paths
Routing
Routing history
Security

ABSTRACT

Mobile Adhoc Networks are shortly called MANETs. In these types of networks, fixed infrastructures are absent and are dynamic in nature. Nodes are movable, and they are not connected with any wires. For monitoring or supervising the transmissions in MANETS, no central supervision is present. Moving nodes, dynamic topology, and absence of infrastructure are the features of MANETs. These features are advantageous where wires cannot be used and where nodes are supposed to move. But there is a problem of security. Networks are highly prone to attacks where finding the root of the cause is very hard. Many nodes disjoint routing algorithms are proposed to balance the load, to cope up with link failures, etc. This paper proposes an algorithm called Node Disjoint Random and Optimal Path Selection (NDROPS) algorithm which uses the concept of dynamic routing and node disjoint routing to provide all the above-stated advantages along with security. Routing of data packets is done through few paths which are node disjoint. The main essence of this algorithm is to distribute the data among different routes. So, a malicious node in a path can retrieve only a few packets in random. The simulation of the proposed NDROPS algorithm is performed and the performance is compared using throughout and packet drop probability.

Corresponding Author:

P. Suma
KL University,
Guntur, India.
Email: sumapatra@gmail.com

1. INTRODUCTION

A network with moving nodes and changing topology can be called a MANET. All the individual nodes in mobile ad-hoc network (MANETS) functions as routers. The support for mobile nodes connectivity and wirelessness are the best characteristics of MANETS. Due to these features MANETS are widely needed where wires and central monitoring system cannot be established. The application fields which require moving nodes attract MANETs. The nodes in a network k must move within the boundary. So, the nodes which cross the boundary out will be removed from the network and nodes are also included when they come in to the boundary. The absence of central monitoring system may cause several attacks. In wired and the networks with central supervision, it is easy to detect the cause of the attack. And this is not the case with MANETs. Till now many measures are proposed to provide security but still there is a need to increase the level of security.

Dynamic routing and node disjoint routing are two distinct routing techniques. These are used to restrict the data transmission in a single path [1], [2]. These types of routing techniques were used to balance the traffic load, handle the situation when some failure occurs in a route etc [3]. This paper proposes an algorithm where paths of transmission are many and are selected in random. In this, the paths selected are

node disjoint.

The content of the paper comprises of History, Areas of application, Negative characteristics, and various challenges of MANETs. Then Advancements till now, the proposed algorithm with notations followed by Conclusion.

2. DEVELOPMENT OF MANETS

ALOHAnet, Packet Radio Networks (PRNET) and Survivable Adaptive Radio Networks (SURAN) are used in the 1970s.

Commercial Adhoc Networks were prevailing in the 1990s and later MANETs are being used.

3. AREAS WHERE MANETS ARE PREFERRED

MANETS are preferred in the areas where wires cannot be used and nodes are needed to be mobile in nature.

Few areas where MANETs are used are,

1. Communication in Military Organizations
2. Battlefields
3. Rescue or searching operations
4. Disaster management and Recovery
5. Outdoor Games
6. Internet while moving
7. Taxies/ cabs
8. Sports stadiums
9. Aircraft or water transport communications etc.

4. NEGATIVE CHARACTERISTICS

Deficiency of Centralized monitoring: A Central supervising system is used to manage the communication in the network and to monitor the security issues. But MANETs are not provided with such system [4]. Many problems arise due to this.

Problem in finding the attacker: Nodes are continuously added and removed from the premises of the network. So detecting the cause for an attack is a hard task [5].

Level of Adapting new nodes: The network must be able to handle and adapt when new nodes enter the network boundary. Absence of this adaptability is a major problem in MANETs.

Node Cooperation: All the nodes must try to cooperate with each other as there is no central supervising system [5].

Unstable network Topology: The positions of the nodes are always changing. So, cooperation, reliable communication is problematic [6].

Limit in Resources: Energy of nodes, Bandwidth and protection from viruses are limited. This causes unreliable communication [7].

Problem in estimation of total Bandwidth in a network: Dynamic topology, addition and deletion of nodes make the estimation of bandwidth hard [8].

Insecurity due to presence of malicious node: There will be no exact information of nodes with an intention to attack the network's security [9].

Compatibility of Protocols used: Protocols used by all the nodes must be supporting to each other for reliable communication [8].

Inexact Boundary of network: The range of border of a network is not appropriate. This creates a problem in data transmission and security in the network.

5. VARIOUS CHALLENGES

Availability of nodes: Nodes must be available to the each other even in the presence of attacks and limited resources etc [9].

Authentication of nodes: The nodes in MANETs must be authenticated for security. This can stop malicious nodes to act as an authenticated one. Authentication of nodes serves to improve security in MANETs [6].

Node Anonymity: Limitations must be there to alter the original information of a person and other routing information [9].

User Authorization: Access rights must be provided to the users to perform some actions [5].

Data Confidentiality: Confidential data must be protected from attackers and unprivileged users [8].

Integrity: Data retrieval and alteration rights have to be given only to the authorized persons to provide integrity of data. This provides security [4].

Non-repudiation: A source and destination must agree the action performed by them. Disagreement later is not encouraged. So, measures have to taken to protect the network from non repudiation [5].

Catch and discard the malicious nodes: Identification of attacking nodes must be done and they must be kept away from involving in the network activities [7].

6. RELATED WORK

Dynamic routing, node disjoint routing strategies was used as a solution for various problems like link failure, finding optimal paths and to balance traffic through all nodes etc. Few such works are stated and referenced below.

Shuchita *et al.* [3] proposed a method of finding node and link disjoint paths to attain few positive qualities. A Node Disjoint Multipath Routing Considering Link and Node Stability (NDMLNR) protocol was proposed to reduce energy loss of few nodes and to work well in link breakages.

Node-Disjoint Multipath Routing Protocol (NDMR) was proposed [10] to mitigate the overhead while routing data. This protocol proposed an agent based Service Level Agreement (SLA management) system to pick a node disjoint path. This is also used to balance the traffic and to cope with node failures.

A multipath routing technique was proposed [11] to handle the link failures in MANETs. Node disjoint paths are identified between the sender and receiver to reduce delay and to attain good throughput levels.

A protocol with multipath routing using Node disjoint paths was proposed to work well in link failures. This technique of routing was meant to reduce packet dropping, delay and efficient delivery of data to the destination [12].

A protocol based on AODV protocol was stated to find three node disjoint paths between sender and receiver. This was done to reduce load on fixed nodes by distributing load on to many nodes [13].

In Node-Disjoint Multipath routing protocol [14] for routing of packets is done by making the nodes disjoint in the network. This type of multipath routing is done to have reliable data transfer in time.

An Efficient Dynamic Route Optimization Algorithm for Mobile Ad hoc Networks [15], is an algorithm to find optimal route. This algorithm can be shortly called DROA. To optimize the route number of hops, delay in traffic, power of nodes were considered.

S.Sharon *et al.* proposed an efficient routing protocol to provide security in data transmission. In this [16], geographical or position based routing is done. Time is a constraint in routing, i.e when time limit is reached, other next hop is chosen for transmission.

Another type of routing technique which is based on Alpha numeric [17] was proposed. Nodes in a network are classified as leader nodes and active nodes, where leaders are used to monitor the active nodes. Data transmission is done only through the nodes which are authorized. This algorithm is specially used to prevent worm hole attack. In worm hole attack a tunnel is established between two attacker nodes and data is transmitted in through this tunnel only.

Back up routing protocol was proposed by S.J Lee *et al.*, [18]. This is based on AODV protocol. When a link failure occurs, alternative path is selected for transmission dynamically.

Node disjoint paths are used in On-demand Multipath Distance Vector Routing for Ad Hoc Networks [19]. In this routing method, many paths are involved for data transmission. Stale path usage can be reduced by the concept of node disjointness.

7. PROPOSED WORK

We propose a random path selection algorithm (NDROPS) to route the data packets through different node disjoint routes in order improve security in MANETS. In general, to send data a path is used for transmission. Any node in this path can read the data. This reduces data confidentiality and security. The present work tries to find node disjoint paths between the sender and receiver using any method proposed by various authors. Each successive packet follows different routes. When all the elected paths are used once, again the successive packets start to transmit through the selected paths again in random. Assume there are 5 node disjoint routes between sender and receiver and 25 packets to be transmitted between them. Only 5 packets are transmitted through each path, that too in random (here and there).

Representative Notations:

a. S is Source
b. D is Destination
c. Set of Node Disjoint Paths between source and destination are denoted as P. Where P = {P1, P2.....Pm}
d. m is total number of disjoint paths between S and D
e. m is also used to denote the size of an array
f. R is an array to store the history of paths taken by data.

To implement this idea, first the total number of node disjoints paths between S and D have to be finalized (Suppose P1, P2 ...Pm).Many algorithms are there till now to find the node disjoint paths. Use any of such algorithm to determine the node disjoint paths.

Declare an array at the source node which is of size 'm'.

Process of sending data: Send the packet1 through any node from P. For suppose it is sent through P3. Then store P3 in R, where R is any data structure of length 'm'. Send the next packet through any paths from P other than the paths stored in R (other than P3). Store the next selected path in R. Repeat this process till all packets are sent or R is full. If all packets are sent, the work is done. If R is full, clear its memory and start the process of sending and continue till the complete message is sent.

If all the packets pass through a single path, there is a chance for an attacker in this route to get all the information. The proposed algorithm uses different paths for data transmission to achieve security. If more number of paths are chosen, we can send the packets through all of them. Then the person at any node cannot hear to the complete data. He can get only few packets of data and that too in random.

Node Disjoint Random and Optimal Paths Selection algorithm (NDROPS):

Steps:

1: Set the nodes
2: Determine the sender node and destination node
3: Find out the different node disjoint paths (P=P1, P2, P3.....Pm) connecting source and destination
4: Declare an array R of size 'm' to hold the history of routes used to transmit packets.
5: Send the packet from any path from p. (Assume as P*x*) and save the path as the first element of the array R.
6: Select a path from P (Assume Py) to send the successive packet and before sending check the history.
7: If the path chosen is already in the array, choose other path apart from the paths in the history and insert that path as a next element of the history array.
8: Repeat Step 6 till the array is full or the data packets are completely sent.
9: If R is full, delete all the contents of the array and go to Step 5.
9: If the complete data is sent, TERMINATE the process.

When varied paths are used to send successive data packets, no person at any node of network can read the data completely. By this many MANET attacks can be prevented. Apart from security, load balancing, reliable packet transmission, handling link failures efficiently, SECURITY can also be achieved using NDROPS algorithm.

Using NDROPS algorithm the following attacks can be prevented effectively.

a. Black hole attack: [20]
b. Byzantine attack: [5]
c. Data Packet Dropping attack: [4]
d. Eaves Dropping: [5]
e. Fabrication attack: [20]
f. Grey-hole attack: [5]
g. Man in the middle attack: [4]
h. Rushing attack: [7]
i. Selective Forwarding attack: [13]
j. Wormhole attack: [6] etc.

8. RESULTS AND DISCUSSION

This section shows the simulation of MANET environment and the experimental results of the proposed NDROPS method for optimal path selection. Then, the proposed NDROPS routing algorithm is analyzed with the attack based NDROPS using the parametric analysis, which has been performed based on the packet drop probability and throughput.

8.1. Simulation Set Up

In this paper, we have used MATLAB software to perform the simulation of mobile ad hoc network using various numbers of nodes. In the simulation, the MANET nodes are fixed in the area of 150mx150m. Then, the performance evaluation is done based on the evaluation metrics.

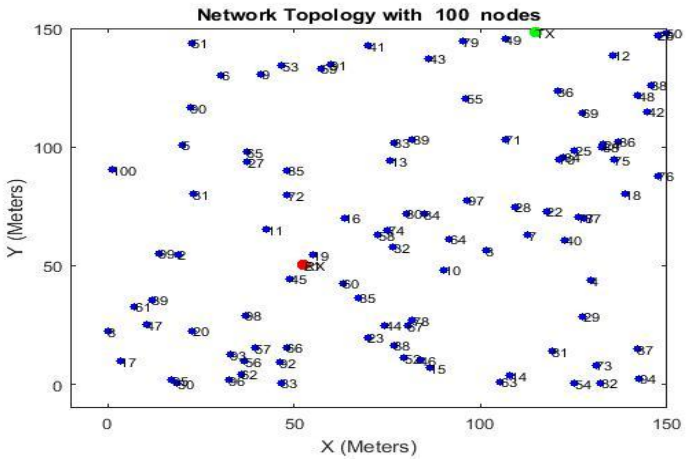

Figure 1. Simulation setup for the NDROPS routing algorithm

8.2. Performance Evaluation

The performance is evaluated based on two different metrics. Throughput is defined as the rate of successful data transmission with respective particular time. Packet drop probability is used to find the probability measure about the loss of packets during the transmission.

8.2.1. Performance Evaluation based on Throughput

The throughput analysis of the proposed NDROPS routing protocol is shown in figure 2. Here, the rate of successful packet delivery is calculated between the two routing protocol named as NDROPS and NDROPS with the attacker nodes. When the transmission time of data is fixed as 3 seconds, the throughput for the NDROPS routing algorithm obtained as 0.97. At the same time, the throughput value of the NDROPS with attack node is achieved as 0.8. Further increasing the transmission time from 2 seconds to 6 seconds, the throughput of the both NDROPS and NDROPS with attack nodes is obtained as 0.95 and 0.25 respectively. Basically, the attackers present in the routing path are used to reduce the throughput value. While fixing the transmission time as 8 seconds, the throughput of the NDROPS protocol and the NDROPS with attack nodes is measured as 0.67 and 0.21 respectively. From the above results, we can say the proposed NDROPS transmit the number of data packets with high throughput.

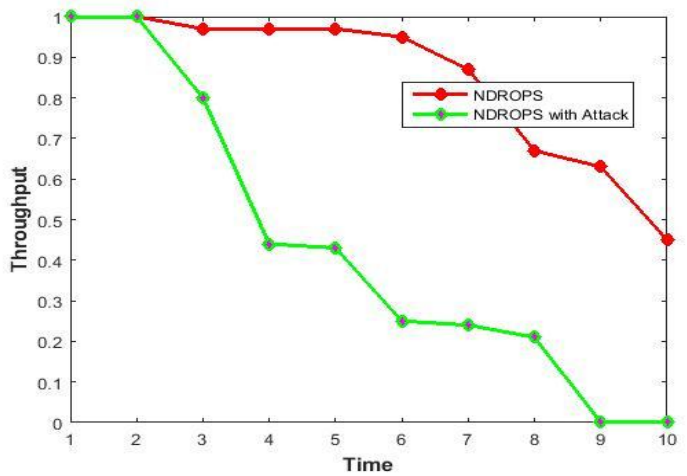

Figure 2. Throughput analysis

8.2.2. Performance Evaluation based on Packet drop Probability

Figure 3 shows the comparison result of both NDROPS and NDROPS with attack nodes based on the packet drop probability. At first, the evaluation of the packet transmission is done without using any attacker nodes. Here, the packet drop probability of the proposed NDROPS protocol is achieved as 0.03, while fixing the time of data transmission is 3 seconds. Meanwhile, the packet drop probability of the NDROPS with attack nodes is obtained as 0.2. When the transmission time is fixed as 6, the packet drop probability measurement of the NDROPS routing protocol is achieved as 0.05. Also, the throughput value of the NDROPS with attack nodes is obtained as 0.75, which is higher than the NDROPS routing protocol. From this figure, we can conclude that the highest performance is achieved by the proposed NDROPS routing protocol without attacker nodes.

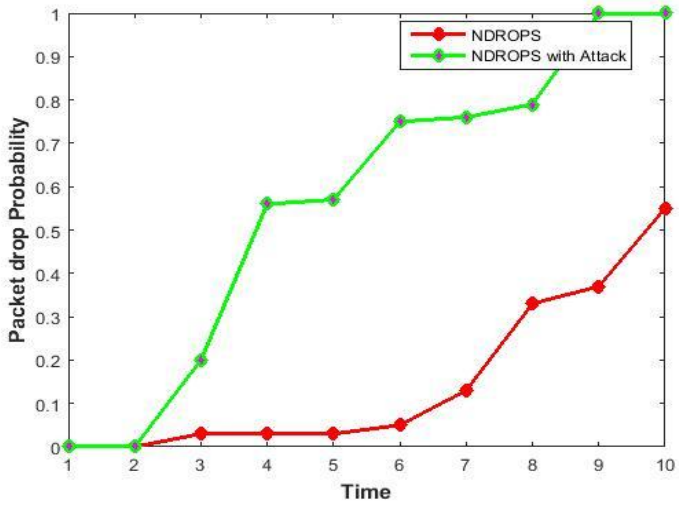

Figure 3. Packet drop probability analysis

9. CONCLUSION

MANETS are widely preferable where there is a need for mobile nodes and where wired connectivity is hard to establish. These networks are very much prone to several attacks due to the lack of supervision system and addition/deletion of nodes in network. Dynamic multipath routing and node disjoint routing in MANETs are useful to balance load, balance resource consumption, ensured transmission of data even in link failures. The Node Disjoint Random and Optimal Path Selection (NDROPS) algorithm is newly proposed in this paper to achieve all the above stated goals along with security. The concept of this algorithm is attack prevention. To prove the performance of the proposed NDROPS algorithm, the comparison is made using throughout and packet drop probability. In future, this work can be extended with an optimization algorithm to provide the robustness against various attacking scenarios.

REFERENCES

[1] Madhumita Kathuria, Sapna Gambhir, "Improvement of Quality of Service Parameters in Dynamic and Heterogeneous WBAN", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 4, no. 4, December 2016.

[2] Kazeem B. Adedeji, Akinlolu A. Ponnle, "Improved Image Encryption for Real-Time Application over Wireless Communication Networks using Hybrid Cryptography Technique", *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 4, no. 4, December 2016.

[3] Dr. Shuchita Upadhayaya and Charu Gandhi., "Node Disjoint Multipath Routing Considering Link and Node Stability protocol: A characteristic Evaluation", *International Journal of Computer Science Issues (IJCSI)*, vol. 7, no. 1, No. 2. 2010.

[4] Zaiba Ishrat, "Security issues, challenges & solution in MANET", *IJCST*, vol. 2, no. 4, 2011.

[5] Manjeet Singh Gaganpreet Kaur, "A Surveys of Attacks in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, 2013.

[6] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", *International Journal of Multidisciplinary and Current Research (IJMCR)*, vol. 2, pp.62-68, 2014.

[7] Godwin Ponsam, Dr. R. Srinivasan, "A Survey on MANET Security Challenges, Attacks and its

Countermeasures", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, 2014.
[8] H. Yang, H. Luo, et al., *"Security in mobile ad hoc networks: challenges and solutions"*, In proc. IEEE Wireless Communication, UCLA, Los Angeles, CA, USA, vol. 11. 38- 47, 2013.
[9] S. Marti, T. J. Giuli, K. Lai, M. Baker, *"Mitigating Routing Mis- behavior in Mobile Ad Hoc Networks"*, Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (Mo- biCom'00) pp.255-265, 2000.
[10] Luo Liu, Laurie Cuthbert, "QoS in Node-Disjoint Routing for Ad Hoc Networks", *I. J. Communications Network and System Sciences*, pp.1-103, 2008.
[11] A. Monisha, K. Vijayalakshmi, "A Reliable Node-Disjoint Multipath Routing Protocol for MANET", *International Journal of Computational Engineering Research*, vol, 03, no. 4, pp. 6, 2013.
[12] Jayshree Tajne, Veena Gulhane, "Multipath Node-Disjoint Routing Protocol to Minimize End To End Delay and Routing Overhead for MANETs", *International Journal of Engineering Research and Applications (IJERA)*, vol. 3, no. 4, pp.1691-1698, 2013.
[13] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", *International Journal of Computer Applications*, vol. 9, no.12, 2013.
[14] Xu Yi, Cui Mei, Yang Wei, Xan Yin, "A Node disjoint Multipath Routing in Mobile Ad hoc Networks", *IEEE*, 2011.
[15] Liang Huang ,Fubao Wang, Guoqiang Yan, Weijun Duan, *"An Efficient Dynamic Route Optimization Algorithm for Mobile Ad hoc Networks"*, 2nd International Conference on Challenges in Environmental Science and Computer Engineering (CESCE 2011), vol. 11, part A, pp.518–524, 2011.
[16] S.Sharon Ranjini, G.Shine Let, "Security-Efficient Routing For Highly Dynamic MANETS ", *International Journal of Engineering and Advanced Technology (IJEAT)*,vol 2, no. 4, 2013.
[17] Rajinder Singh, Parvinder Singh, Manoj Duhan, "An effective implementation of security based algorithmic approach in mobile adhoc networks", Human-centric Computing and Information Sciences, 2014.
[18] S.-J. Lee and M. Gerla, *"AODV-BR: Backup Routing in Ad hoc Networks"*, In Proceedings of IEEE WCNC 2000, Chicago, IL, Sep. 2000.
[19] Marina, M.K., "On-demand multipath distance vector routing in adhoc networks", *Network Protocols, IEEE*, pp.14 – 23, 2001.
[20] Pankajini Panda, Khitish Ku. Gadnayak, Niranjan Panda, "MANET Attacks and their Countermeasures: A Survey", *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 2, no. 11, pp. 319-330, 2013.