INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Cost Optimal Random Path Selection Algorithm for Security in MANETS

P. Suma
Assistant Professor, Department IF IT, KITS Warangal, India
O. Nagaraju
Professor & Head, Department of CS, Government College, Macherla Guntur, India
Md. Ali Hussain
Professor, Department of ECM, KL University, Guntur, India

Abstract:
MANETS are mobile adhoc networks with no fixed infrastructure and is in dynamic nature. Nodes are mobile, connected without wires and they don't have any central supervision. Wireless infrastructure, changing topology, mobility of nodes are advantageous. These qualities of MANET make the network open for many types of attacks at different layer. The main problem is, the detection of the cause of attack and prevention of attacks becomes complex. This paper introduces a dynamic routing algorithm for prevention of many attacks. This algorithm is cost effective and provides secure data transmission.

Keywords*: Manets, attacks, security, minimum cost, routing, history*

1. Introduction

A MANET is a type of network with mobile nodes. Each node in this mobile adhoc network works as a router. The moving capability of nodes, wireless facility, and best connectivity with other moving nodes of the network makes MANETs very attractive. These facilities made the need for MANETS increase enormously. The areas where moving nodes are desirable wish to use this type of network. When all the nodes in a network are in motion, many nodes are added and many gets discarded from the network for various reasons. Especially there will be no centralized monitor to manage the nodes. This dynamic behaviour lead to various attacks. Compared to the networks, with immovable, wireless and wired nodes, Mobile Adhoc Networks are highly prone to many types of attacks. Though many techniques and theories were proposed to increase the security in MANETs, there is still a need to improve security for the data in transmission.

Dynamic and multipath routing are routing techniques where data transmission is not done in a single fixed path. By taking different criterion into consideration routing of packets is done through multiple routes. In this paper a random path selection algorithm is proposed by considering the cost.

The rest of the paper includes the Evolution of MANETs in Section II, Application of MANET in Section III, Weak Aspects in Section IV, Security and Reliability Challenges in Section V, Existing work in Section VI, Proposed solution in Section VII followed by Conclusion and Future Scope of Research in Section VIII.

2. Evolution of MANETS

Period of Time	Name of network
Early 1970's	ALOHAnet
1970's	Packet Radio Networks (PRNET)
1970s	Survivable Adaptive Radio Networks (SURAN).
1990s	Commercial Adhoc Networks
At present	Mobile Adhoc Networks (MANET)

Table 1

3. Applications of MANET

MANETS are applied where there is a need for mobile nodes and wireless infrastructure [vi].
Following are few application areas of MANETs

1. Military communications
2. Automated battlefields
3. Search and rescue operations
4. Disaster Recovery Management when Earthquakes and Hurricanes etc. occur
5. Multi User Games
6. Outdoor Internet access
7. Taxi cab network
8. Sports stadiums
9. Boats, small aircraft
10. Policing and Fire fighting etc.

In all these areas MANETs work efficiently.

4. Weak Aspects

- Absence of Centralized Supervision: MANETs doesn't have any central management system to manage the communications in a network [x]. This leads to a problematic situation in maintaining security.
- Detection of Malicious Node: A Node can be connected or disconnected randomly in the MANETs. Malicious nodes also get into the network whose detection becomes very hard [vi].
- Adaptability: The network must have a capability of getting enlarged to have room for the newly attached nodes. Lack of this capability shows impact on security [x].
- Cooperative Nodes: The movable nodes in a MANET must be more cooperative to all other nodes when compared to a static network due to their mobility and other constraints [vi].
- Ever Changing Topology: The reliability between the nodes gets reduced or disturbed due to the changing positions of each node [xv].
- Low Resources: Resources like power supply, virus protection etc is very limited. This leads to low security levels [ix].
- Limited Energy Levels: The nodes with low power are less often selected in routing through them. If the power or energy exhausts, link between few nodes gets delinked [xi].
- Estimation of Bandwidth Constraint: As the links in a network change, the estimation of bandwidth or the data rate becomes difficult [xiv].
- Insecure Surroundings: Random movement enables any malicious node to enter the environment which may cause theft of data [xi].
- Compatibility of Security Protocols: Protocols for providing security in wired networks are not suitable for Wireless and Adhoc Networks [xiv].
- Inaccurate Boundary: A border line of the network range can't be established accurately. Nodes can be attached or detached from this mobile network. This becomes a security problem [vi].

5. Security And Reliability Challenges

- Availability: Data and the resources must be accessible even if some attacks prevail like DOS attack, presence of malicious node, low energy constraint etc. This is important while working with Mobile Adhoc Networks [xi].
- Authentication: The nodes in a network must be identified uniquely. Else, any node which is malicious can pretend as the identified one. Due to lack of authenticity, data insecurity may occur [xv].
- Anonymity: All the personal details of a person who uses a device in a network must not be modified by any person or software including him [xi].
- Authorization: It is the process of giving access rights to a user to perform various activities and to use different resources etc [vi].
- Confidentiality: It is to provide certain privacy to users in protecting their data against unprivileged users. It is secrecy of information [xiv].
- Integrity: Data reading or modification must be done only by the persons who are authorized. It is a crucial security issue [x].
- Non-repudiation: A sender or a receiver must not say that the activity performed was not actually done by him. So, some security technique has to be implemented to prevent such disagreements [vi].
- Finding and Removing: Misbehaving nodes have to be identified in time and have to isolate it from network [ix].

6. Related Work

Till now, the dynamic routing technique has been used as a solution for many problems.

It is used to select an alternative route when a route is busy or broken, to select a best path considering many criterion like high power, quality, less prone to breakage etc. Dynamic routing is used for security, balancing the load also.

In Node-Disjoint Multipath routing protocol routing [ii] 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.

In a paper, “An Efficient Dynamic Route Optimization Algorithm for Mobile Ad hoc Networks” [i], an algorithm for route optimization named DROA was proposed. Nodes in MANETS are mobile. Though the topology of the network changes continuously, best path is selected for transmission. This selection of path is based on hop count, traffic, delay, energy etc.
S.Sharon et al. [iii], proposed a secure and efficient routing protocol to deliver the data packets. This used geographical routing or position based routing. Data is sent to destination using the next hops. This selection of hops is based on trust value. If the selected path fails to send data within stipulated time, other hops are selected.
In an algorithm, “Alpha numeric based secure reflex routing” [iv], the nodes in MANETs are qualified as leader nodes and active nodes. Leader nodes are responsible to verify the access nodes attached to it. Data is transmitted through the nodes which are authorized. This algorithm is proposed to prevent wormhole attack by routing the data packets via leader nodes (LN) and access nodes (AN) which are authorized.
S.J Lee et al, [v], proposed a protocol based on AODV called Backup Routing in Ad Hoc Networks. Here dynamic routing concept is used when link failure occurs.
In a paper, “On-demand Multipath Distance Vector Routing for Ad Hoc Networks” [viii], multiple paths are chosen by considering node disjointness i.e. Nodes must not be repeated in a path. This is also to reduce the usage of stale paths.

7. Proposed Work

We propose a random path selection algorithm to route the data packets through different routes in order improve security in MANETS and mainly with in the cost limit. When packets are sent from source S, a path is selected in order to reach the destination D. Any node in that path will have a chance to retrieve the sensitive data. This leads to the loss of security. Our idea is to choose some number of different paths for the packet transfer. So that, at any node the complete data cannot be retrieved.

7.1. Notations

- Source→S
- Destination → D
- P = (P1, P2.........Pm) → Paths between source and destination.
- m → total number of paths between S and D
- x → some integer (used in % increase).
- *p = (p1,p2,....pn)* → Paths within the limit of cost
- n → number of paths in *p*.
- R → data structure to store the history of paths taken by data.

To implement this idea, first the total number of paths between S and D have to be finalized (Suppose P1, P2 ...Pm).
Calculate the cost for each path using some algorithms which are developed till now. Then find out the path with minimum cost out of them. Assume that P4 is the path with minimum cost (suppose 150units). Then determine how much percentage increase to the minimum cost can be affordable. Assume 25% of increase to the minimum cost is affordable. 25% more to 150 is 150+37 i.e.187. Now identify the paths (*p=p1, p2....pn*) whose cost is less than 187units. If n<4, increase the affordable increase of cost and estimate the paths within the limit of cost again. Do this, to increase the number of paths supporting the data transfer. If the paths are less many number of packets pass through a single path and there is a chance for an attacker to get much information. This makes our algorithm to achieve security and reduce the cost, though we don’t choose the shortest path.
If more number of paths are within the limit of cost, 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.

→ 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 n. 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.

7.2. Cost Optimal Random Paths Selection algorithm (CORPS):

- Step 1: Initialize the nodes
- Step 2: Initialize the source and destination
- Step 3: Identify the different paths (P=P1, P2, P3......Pm) connecting source and destination
- Step 4: Calculate the cost of each path with some existing algorithm.
- Step 5: Find the least cost path.
- Step 6: Finalize the affordable %increase in the minimum cost (x% more than the minimum cost).
- Step 7: Identify all the paths whose cost is within the limit. Name them as “least cost paths (*p=p1, p2, p3......pn*)”.
- Step 8: If n<4 go to Step 6 to increase the affordable % of minimum cost.
- Step 9: Declare a data structure R of size 'n' to store the history of paths taken by each packet.
- Step 10: Send the packet 1 through any path (*px*) in random and store the path as the first element of R.

- Step 11: Send the next packet through any path apart from the paths in the history and insert that path as a next element of the history.
- Step 12: Repeat Step 11 till R is full or all the packets are sent.
- Step 13: If R is full, delete all the elements form R. and go to Step 11.
- Step 14: If all the packets are sent, STOP.

When much number of paths are chosen for the transfer of packets, maximum number of attacks on MANETS can be prevented. Following is the description of the MANET attacks which can be overcome using CORPS algorithm.

- Black hole attack: An attacker proposes the sender that some route is the shortest route to the destination. By this lie, the confidential data packets are heard at a malicious node in that shortest route [ix]. If different paths are randomly chosen, Black hole attack can be prevented.
- Byzantine attack: Few nodes attack the network by creating loops, so that data is looped between few nodes or sent through unwanted paths [vi].

If the proposed algorithm is applied along with loop prevention algorithm, one can overcome Byzantine attack.

- Data Packet Dropping attack: The nodes between the sender and destination are used in routing the data packets. A malicious node in the path may drop the packets without transmitting it further [x].

This attack can be prevented using the proposed algorithm.

- Eaves Dropping: In a MANET, the data sent from source to destination takes multiple hops. The data can be retrieved at each intermediate node if it is not encrypted. This retrieval of sensitive data is called Eaves Dropping [vi].

If multiple paths are selected for packet transmission eaves dropping can be eliminated.

- Fabrication attack: This attack is focused on wrong routing. It shows that the next hop node is unavailable, so that the packet has to travel through unoptimized route [xii].

If a node is shown unavailable, other paths from *p* can be selected. Thus we eliminate fabrication attack.

- Grey-hole attack: In it, a node shows an inefficient route as a valid one and drops the packets passing through it [vi].

When CORPS algorithm is implemented many paths are selected and packets are transmitted through them. Few packets passing through this malicious node may be dropped but they can be retransmitted.

- Man in the middle attack: A node between the source and the destination node retrieves the data that is communicated by them [x].

When the proposed algorithm is used, a man in middle cannot get complete data.

- Rushing attack: In this attack, Route discovery request is captured by an attacker and gives reply very fast when compared to the other nodes. This route contains the node where an attacker is present [ix]. The transmission of data packets is done through this route. Then tapping the data is done easily.

If the present algorithm is used, though one route is shown as best, multiple routes have to be utilized. Thus we prevent rushing attack.

- Selective Forwarding attack: In Selective forwarding attack, a malicious node pretends to be legitimate and it drops the data packets randomly and forwards few of them [xiii]. Choosing many routes can eliminate this attack.
- Wormhole attack: Pair of malicious nodes colludes and one of its node routes the data packet to its paired node through a tunnel. The tunnel between the colluded nodes is said to be a worm hole [xv].

Though a tunnel is formed, only few packets move through it as we use CORPS algorithm. Rest of the packets reach the destination safe.

8. Conclusion and Future Work

Though MANETs result in many attacks, they are widely used due to wireless nature and mobility of nodes. Many security attacks were discovered and few solutions were also proposed. Many are still to be known. This paper provides a dynamic routing algorithm which is cost effective and provides security of data while in transit in a MANET. Many MANET attacks can be prevented using the proposed algorithm CORPS.

We further can develop dynamic routing algorithms to provide security in MANETs by taking some other constraints like energy, cost, number of hops etc.

9. References

i. 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 Environmenta l Science and Computer Engineering (CESCE 2011), Volume 11, Part A, PP.518–524, 2011.
ii. Xu Yi, Cui Mei, Yang Wei, Xan Yin, “A Node disjoint Multipath Routing in Mobile Ad hoc Networks”, IEEE,2011.
iii. S.Sharon Ranjini, G.Shine Let , “Security-Efficient Routing For Highly Dynamic MANETS “, International Journal of Engineering and Advanced Technology (IJEAT),vol 2, issue 4, 2013.
iv. Rajinder Singh, Parvinder Singh and Manoj Duhan ,”An effective implementation of security based algorithmic approach in mobile adhoc networks”, Human-centric Computing and Information Sciences, 2014.
v. S.-J. Lee and M. Gerla, .AODV-BR: Backup Routing in Ad hoc Networks, In Proceedings of IEEE WCNC 2000, Chicago, IL, Sep. 2000.

vi. Manjeet Singh1 Gaganpreet Kaur, "A Surveys of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 6, 2013.

vii. K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, "A secure routing protocol for Ad Hoc Networks," in Proceedings of ICNP'02,2002.

viii. Marina, M.K., "On-demand multipath distance vector routing in adhoc networks", Network Protocols, IEEE, pp.14 – 23, 2001.

ix. 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). Volume 3, Issue 1, 2014.

x. Zaiba Ishrat, "Security issues, challenges & solution in MANET" IJCST. Vol. 2, Issue 4, 2011.

xi. 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.

xii. 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 Issue 11, pp. 319-330, 2013.

xiii. Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications. Volume 9– No.12, 2013.

xiv. 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. Volume- 11. 38- 47, 2013.

xv. Sachin Lalar., 2014. Security in MANET: Vulnerabilities, Attacks & Solutions. International Journal of Multidisciplinary and Current Research (IJMCR), Vol.2, pp. 62-68, 2014