A Survey on Security Schemes for Multipath DSR routing

Dr. Anna Saro Vijendran [1] J. Viji Gripsy [2]

Abstract:

MANET is an infrastructure fewer networks composed of mobile nodes. Link failure due to node mobility increases the necessity of multipath routing in MANET. It improves reliability, robustness and load balancing. There are numerous routing protocols in MANET classified under two major categories, such as Topology based and Position based, on which DSR comes under Topology category that is widely considered as simplest protocol for routing. Multipath technique is used along with most of the routing protocols to overcome route failure drawback of single path. Wireless links in MANET made security an inevitable process. Malicious node tends to compromise the nodes within network to launch attack. This entity could lead to significant vulnerability. The focus of this paper is on surveying various schemes adopted for reducing vulnerability issues in DSR.

Keywords: MANET, Multipath DSR, Attacks, Security schemes.

1. Introduction

Ad-hoc networks are new wireless network that recently used in mobile hosts. Ad-hoc network is not a new concept it's derived from dynamic wireless network. As it is a self organizing network, does not encompass any central organizer like base station or mobile switching centres and its topology changes dynamically because it cannot ensure whether the mobile node continuously stay in one place.

MANET is composed of multi hop mobile nodes that make use of wireless link to communicate. There are two types of MANET namely Open MANET and Close MANET. In Open MANET nodes does not depend upon any infrastructure like Wi-Fi but moves around randomly within the network range. Central authority in wired network rules over network topology. In case of Wireless network, any node can join or leave the network at any time. In Recent years, many researches focus on reducing the security challenges faced by Mobile Ad-hoc network. In MANET concentration should be possessed on issues in different layers such as Security issue in Application layer, QOS issue in Transport layer, Routing issue in Network layer and power control issue in Physical and link layer. Routing in MANET plays vital role in the security of entire network. Routing protocols have to find routes for packet delivery and make sure the packets are delivered to the correct destinations. Mobile nodes communicate via wireless interface such as air because of which security becomes a very important issue. Mobiles nodes are freely accessible and not protected at all so wireless link can be intercepted or disrupted by an attacker more easily. MANETs are highly vulnerable for passive and active attacks as node mobility makes it hard to determine which node really left the network, has been intercepted or blocked due to malicious activity or just changed the location. In design of network the main challenge is on vulnerability. To avoid vulnerability, there is a need for attention on security of data transmission and route discovery. Therefore, many mechanisms and protocols have to be developed to secure MANETs. In general, routing security in wireless MANETs appears to be a problem that is hard to solve.

The rest of the paper is discussed as follows. The next section discusses about DSR. Section III describes Multipath in DSR.

Section IV deals with routing problems associated with MANET. Section V describes attacks in DSR. Some existing Security based multipath DSR routing protocols is described in section VI. Finally, section VII offers conclusion.

2. Dynamic Source Routing

Dynamic source routing [1] is designed for the purpose of source routing. It is a reactive protocol developed by Johnson et al. in 1996. Main advantage of developing DSR protocol is to provide simple, flexible and correct routing. It allows loop-free packet routing that avoids need of continuous update in intermediate node routing table. Reactive protocols find a route to the destination only when there is a need to transmit data from source node. Transmission of a significant amount of control traffic is mandatory when source node tends to find route to destination. DSR protocol is composed of two main mechanisms namely Route Discovery and Route Maintenance. Source node initiates Route Discovery, if it does not possess route to destination in prior. In Discovery mechanism, source node perform global flood search in which Route Request (RREQ) is broadcasted throughout the network. Route Maintenance mechanism plays vital role in MANET as there is dynamic change in network topology. It aids source node with many alternative routes, in case of sudden route failure. If path is not available route discovery mechanism is initiated.

3. Multi path in DSR

In recent scenario wireless network play major role in communication domain than wired networks. Single path transmission is affected by some characteristics of MANET such as dynamic topology, limited battery power and limited channel bandwidth. Because of these characteristics, wireless links are unstable, making communication over ad hoc network difficult. Mobile nodes in MANET can be connected in an arbitrary manner, that helps to establish more than one path between source and destination which has given rise to multi-path transmission. Load balancing and route failure protection can also be provided by multi-paths. Route failure is protected by distributing traffic among a set of disjoint paths. There are two schemes under which paths can be disjoint (1) link-disjoint and (2) node-disjoint. Link-disjoint scheme possess one or more common node but it do not contain common link. Node-disjoint scheme do not possess any node or link in common. This scheme could be embedded into routing protocols according to the need of application.

Advantages of Multipath Routing (MR) [8]

1. MR contains alternative routes from source to destination which makes protocol to be fault tolerant.
2. MR diverts traffic through alternative path in case of congestion which makes protocol to be load balancing.
3. If node possessing low-bandwidth needs to transmit large amount of data then MR splits data packet into multiple stream through Bandwidth aggregation.
4. Delay caused by route failure is reduced in MR.

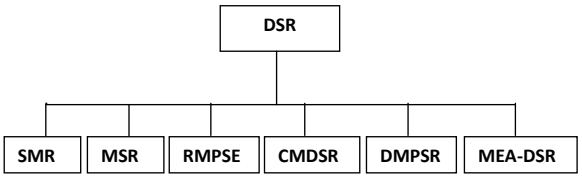

Fig.1. Multipath protocols based on DSR

4. Routing problems associated with MANET

MANET is not controlled by central authority so there is no strict policy for supporting end-to-end routing. Generally, nodes communicate using wireless links which is susceptible to signal interference, jamming, eavesdropping and distortion. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and

distort them to manipulate routes. Major security problems associated with MANET are Selfish, Malicious Behaviour of nodes and Information leakage [7]. Selfish node [10,11] uses network and its service but they do not co-operate with other nodes. Malicious node does not follow the exact behaviour that may redirect the network traffic, modify the message or not forward the message. Two malicious nodes could create wormhole attack [12, 13]. Information Leakage may help intruders to decide about whether, how and when to attack. Routing protocols should be well adopted to handle such problems. Various routing attacks and countermeasures in MANET are surveyed in [9].

5. Attacks on DSR

DSR routing protocol do not possess any security measure in general. So, few attacks occurred in DSR are Dropping of packets, black hole attack, wormhole attack, not sending route error packet, misrouting packets, reducing TTL value of a packet, frequent RREQ creation increases bandwidth consumption etc.

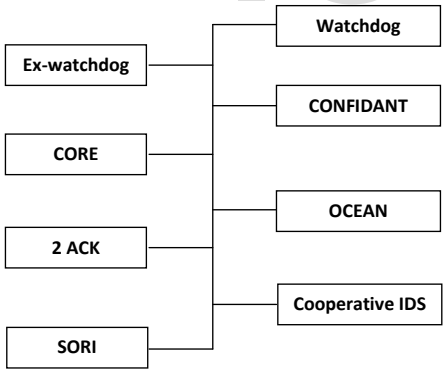

Fig.2. Security techniques against selfishness with DSR

6. Existing Security based multipath DSR routing protocols

Trust based Security [2]

Trust is divided into two kind's namely direct trust and recommendation trust. In direct trust, node trusts another node directly using past experience. Recommendation trust is called referral trust, here one node can trust another node based on the trust information gained for some third entity (node). In [11] trust categories and trust values are used to find different levels of trust. The integral trust values in the model vary from -1 to 4 representing distinct levels of trust from absolute distrust (-1) to absolute trust (4). Here each node stores their trust level which is assigned dynamically to improve the performance of the routing protocol. When node joins the network its trust value is assigned as 0 and it keeps on increasing based on the node's behaviour.

Initially message is divided into different parts, after which each part is encrypted. This encrypted message is transmitted in a multiple paths that have been selected using trust defined strategy. According to this strategy, node with high trust level is given more number of encrypted packets for transmission. Only the destination could decrypt the packets in correct sequence. Secure Route is selected from list of routes based on the trust value of each node involved in hat route. Higher value of trust compromise would increase the probability of message to be broken by a attacker node. So, trust compromise in this paper is zero. Trust compromise value in DSR extends up to 14, which could be easily compromised by an attacker node. Trust based approach is implemented and appended with DSR routing protocol for overcoming three issues such as message confidentiality, message integrity and access control.

Resilient security framework [3]

In this paper, resilient security framework for multipath Ad hoc networks is designed that provides end-to-end security between the Source (S) and Destination (D). Its main goal is to provide security for both multipath routing and data transmission. Multi signature scheme along with a self-certificate technique is used for the provision of secure multipath routing and Schnorr signature algorithm along with the IDA technique is used for the protection of data

integrity during transmission.

When a node joins the network, it needs to get self-certified key from CA (certificate authority). Each node in network contains public key of CA and public parameters of other nodes.

In discovery phase, self-certified key technique is used for key management and multi signature is used for authentication. RREQ is broadcasted along with self-certified signature. Using signature verification algorithm destination node verifies the correctness of signature of source node and its certificate. If match is not found then D does not respond to RREQ else D generate an accumulated route along with partial multi-signature. In Data transmission phase, IDS divides messages into multiple fragments after encryption. Each encrypted message is concatenated with signature and hash fragment. If m fragments are no received before time expiry then D sends ACK for received message fragment else D initiate's data recovery. Proposed scheme along with DSR routing protocol protect against some of active attacks such as message modification, fabrication, man-in-middle attack, black hole attack, invisible-node attack.

Statistical Analysis Approach [4]

In Wormhole Attack [14], attacker fix a point (node) in the network from which it forms a tunnel to another node and starts replay of recorded packets into the network from that point. In this paper statistical analysis (SAM) is proposed to detect wormhole attacks and identify malicious nodes.SAM detects wormhole attack by observing dynamic change in statistics of discovered routes. This statistic value is used to detect the type of routing attacks. Most of the route obtained from route discovery process will contain the link that comes under wormhole attacker tunnel.

To detect wormhole attack in routes some statistics examined are relative frequency of each link in the route, difference between most frequently used link and second most frequently used link. Main steps involved in the proposed scheme for wormhole attack detection are

1) Routes are obtained from Route discovery process on which statistical analysis is performed. If the result detects anomalous pattern then go to step 2 else choose several paths to feedback to the source node.
2) Suspicious paths are tested by sending (test) data packets.
3) Wait for ACK.
3) If ACK is not obtained within TTL of the packet then attack is confirmed.
4) Report to security authority and notify the source and the neighbours of the attackers in order to isolate the attackers from the network.

Generally statistical analysis is the tool to detect routing anomaly in the routes obtained from multipath routing. The malicious nodes can be identified by the attack link which has the highest relative frequency. Some advantage of SAM is it introduces low overhead and it can work with dynamic network topology.

Watchdog approach [5]

In this paper Secure Multipath Routing Algorithm for Mobile Adhoc and Sensor Networks
is proposed which generates set of paths based on disjointness threshold. This value depends on sensitiveness of the data to be transmitted. On-demand property of DSR allow multipath routing algorithm to minimize overhead by specifying path-disjointness threshold. It makes use of six kind of datagram's such as RReq , RRep, Notification, List forwarding, RErr, and Threshold tuning datagram. RReq and RRep works in as usual where as Notification is used to trigger intermediate nodes to send routes it has learned to source node. List forwarding helps in forwarding routes to source node from common intermediate nodes. RErr is send to source when route failure is detected. Threshold tuning is used to dynamically vary threshold value.

To protect against several type of routing attack and wormhole attack watchdog technique [6] is used which detects whether neighbour nodes forward datagram as expected. False routing is protected using digital signature scheme which authenticates

nodes and guarantee integrity of information. Main advantage of Watchdog is that it improves the capability of the node, by allowing it to detect attacks using local information.

	Ref [2]	Ref [3]	Ref [4]	Ref [5]
Base protocol	DSR	DSR	DSR	DSR
Multipath	Y	Y	Y	Y
Security	Y	Y	Y	Y
Security mechanism	Trust based	Resilient security framework	Statistical analysis approach	Watchdog

Table 1: *Different security techniques used in multipath DSR*

7. Conclusion

This paper reviewed various security schemes that are used along with multipath DSR routing protocol. Trust based security, Statistical Analysis Approach, Resilient security framework, watchdog approach are security schemes whose objective is to provide trustworthy routing, detecting (or) eliminating misbehaving and selfish nodes. Thus it is concluded that Multipath DSR contains security mechanism, to ensure the quality of performance still more validations and techniques are required. Watchdog mechanism was recently reviewed and updated by Bayrem Triki et.al [5], to be address for future work.

Reference:

[1] Bayrem Triki, Slim Rekhis, and Noureddine Boudriga, "Threshold Based Multipath Routing Algorithm in Mobile Adhoc and Sensor Networks", Springer, E-Business and Telecommunications, Volume 222, 2012, pp 54-70, 2012.

[2] Binod Vaidya, Dimitrios Makrakis, Jong Hyuk Park,Sang-Soo Yeo, "Resilient Security Mechanism for Wireless Ad hoc Network", Springer Science+Business Media, Wireless Personal Communications, Vol 56, Issue 3, pp 385-401, 2011.

[3] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of computing, vol 3, issue 1, 2011.

[4] MinJi Kim , Muriel Medard , Joao Barros,"A Multi-hop Multi-source Algebraic Watchdog", IEEE Information Theory Workshop, 2010.

[5] P. Narula , S. K. Dhurandher , S. Misra and I. Woungang "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing", *Sci. Direct Comput. Commun.*, vol. 31,pp.760 -769 2008.

[6] Jack Tsai and Tim Moors, "A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks", Workshop on Wireless Multihop Networking, 2006

[7] Frank Kargl, Alfred Geib, Stefan Schlott, Michael Weber, "Secure Dynamic Source Routing", IEEE System Sciences, 2005.

[8] N. Song, L. Qian, and X. Li, "Wormhole attack detection in wireless ad hoc networks: a statistical analysis approach," in Proc. of IEEE IPDPS,2005.

[9] P.Kyasanur, and N. Vaidya, "Detection and Handling of MAC layer MISbehavior in wireless networks, "Int. Conf.on Dependable Systems and Networks (DSN'03), 2003, pp.173-182.

[10] J. Kong, H. Luo, K. Xu, D.L. Gu, M. Gerla, S. Lu, Adaptive security for multilayer ad-hoc networks, Wireless Communications and Mobile Computing 2 (5)pp.533–547, 2002.

[11] L. Blazevic, L.Buttyan, S. Capkum, S. Giordano, J. Hubaux, and J.LeBoudec, "Self- organization in mobile ad-hoc network: The approach of terminodes, : IEEE Communications Magazine, Vol.39, no.6, pp.166-174,2001.

[12] D. B. Johnson and D. A. Maltz, "Dynamic source routing in adhoc wireless networks," *Mobile Computing, T. Imielinski and H. Korth, Eds., Kluwer*, pp. 153–181, 1996.

Y. HU, A. Perrig, and D.B.Johnson,

Packet leashes: A defense against wormhole attacks in wireless networks, "in Proc.22th Annual Joing Conference of the IEEE Computer and Communications Societies (INFOCOM'03), Pittsburgh, PA, USA, vol.3 2003, pp.19 76-1986.

AUTHORS

1. Dr. Anna Saro Vijendran is the Director – Department of Computer Applications in SNR Sons College, Coimbatore, India. She has a teaching experience of 20 years in the field of Computer science. Her area of Specialization is Digital Image Processing and Artificial Neural Networks .She has presented more than 30 Papers in various Conferences and her research works have been published in International Journals. She is currently a Supervisor for research works of various Universities and also act as a Reviewer for reputed Journals.

2. J. Viji Gripsy M.sc., M.Phil., is an assistant Professor in the Department Of Computer Science in PSGR Krishnammal College,Coimbatore, INDIA. She is having a teaching experience of 7 years in the field of Computer science. Her area of Specialization is Security in Adhoc Networks. She has presented more than seven Papers in various International, National & state level Conferences. Also she has published four international journals. She is currently pursuing her PhD Degree under the guidance of Dr. Anna Saro Vijendran in SNR Sons College, under Bharathiar University, Coimbatore. INDIA.

MAIL: gripsyjebs@gmail.com