A Method to Improve the Performance of endairA for MANETs

Vijender Busi Reddy[1,2], M. Ranjith Kumar[1], Atul Negi[1], and S. Venkataraman[2]

[1] Department of Computer and Information Sciences, University of Hyderabad,
Hyderabad, India
[2] Advanced Data Processing Research Institute, Secunderabad, India
{vijender,kalka}@adrin.res.in, ranjithkumar.mitt571@gmail.com,
atulcs@uohyd.ernet.in

Abstract. Mobile Ad-hoc Networks (MANETs) are self-configurable and self-reliance networks. Due to this these networks are vulnerable to routing attacks. *endairA*[6] is one of the secure on demand routing protocol for MANETs. In *endairA*[6], an intermediate node verifies all the signatures carried by the route reply which is a big computational overhead and expensive in terms of power consumption, end-to-end delay. We propose a new approach Impro_endiarA, which will verify at most two signatures at every intermediate node. Proposed approach is efficient in terms of power consumption, end-to-end delay and mitigating some attacks which are possible on some variants of *endairA* [6].

Keywords: Ad-hoc, Security, Routing, endairA.

1 Introduction

MANET forms network in the absence of base stations. The requirement of MANET is just to have mobile nodes that can interact with each other and route the traffic using some routing protocol. Security in MANETs is an essential component for basic network functions like packet forwarding otherwise network operations can be easily jeopardized. Different secure routing protocols are proposed for MANETs each has their own strengths and weaknesses. *endairA*[6] is one of the secure on demand routing protocol for MANETs. In this paper we proposed a new approach to improve the performance of *endairA*[6] protocol.

This paper is organized as follows. Related work is presented in Section 2. Section 3 describes the proposed method. Results are described in Section 4. Finally, section 5 concludes the paper.

2 Related Work

There has been considerable work for securing the MANET routing protocols. ARAN [8] uses previous node signature to ensure the integrity of routing messages. ARAN needs an extensive signature generation and verification during route request phase.

V.V. Das and J. Stephen (Eds.): CNC 2012, LNICST 108, pp. 228–232, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

Secure Routing protocol (SRP) [8] [10] uses secret symmetric key to establish secure connection. Security Aware Ad-Hoc Routing (SAR) [8] provides level of security to share a secret key. SAR may fail to find a route if some of the nodes in the path do not meet the security requirements. Ariadne [12] adds digital signatures to route request which will be verified only at the destination. An attack on SRP and Ariadne is explained in [1].

endairA [6][10] signs route reply message. A practical problem of the basic *endairA*[6] protocol is that each intermediate node verifies all the signatures in the route reply which is too expensive in terms of power consumption and end-to-end delay. To overcome the drawback of *endairA*[6], variant of *endairA* [6] was proposed. In variant of *endairA* intermediate node verifies only Destination signature. Source of route verifies all the signatures in the route reply. This may lead to successful attacks that are clearly explained in [6].

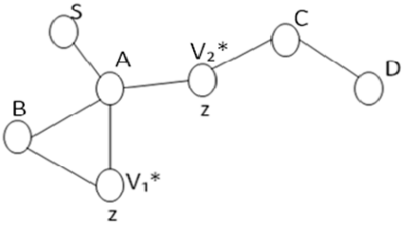

Fig. 1. A configuration of MANET network

3 Proposed Approach

The source of the route generates and broadcasts route request. Once the route request reaches the destination it generates route reply. The route reply contains the source identifier, destination identifier and the accumulated route obtained from the route request. Destination calculates the signature on the above elements appends it to the route reply and forwards it to the next node present in the route. Each Intermediate node in the route receives the route reply and verifies whether its identifier is in the node list, the adjacent identifiers are belongs to neighboring nodes, number of signatures in the reply is less than or equal to number of nodes in the node list and validates two signatures in the route reply message i.e. two hop neighbor's signature and the destination signature. If all these verifications are successful, the intermediate node attaches its signature and forwards the route reply message to the next node present in the node list otherwise the node drops the route reply.

When the source node receives the route reply it verifies whether the first identifier in the route reply is belongs to neighbor and validates all the signatures in the route reply. If all these verifications are successful, the source accepts the route otherwise rejects the route.

Proposed approach, Impro_endairA overcomes the attack on variant of *endairA*[6] which is explained in [6]. Consider configuration in Fig 1[6], Assume that the source is *S*, destination is *D*, and the route reply contains the route (A, B, Z, C). After receiving the route reply from *C* the adversarial node V_2* can send the following message to *A* in the name of *B*.

(rrep, S, D, id ,(A,B,Z,C),(sigD,sigC,sigZ))

A will not accept this message, as it verifies sigC with *Z*'s key which will fail. So the Impro_ endairA overcomes the specified attack in [6] by dropping the route reply packet at node *A* itself.

3.1 Mathematical Analysis of Proposed Work

During the route reply propagation from destination to source, *endairA* verifies one digital signature at the first intermediate node, two signatures at the second intermediate node and similarly n signatures at the *nth* intermediate node. If source is *n* hop distance from the destination, the total number of signature verifications done in whole path from source to destination is:

$$1 + 2 + 3 + \ldots + n = n(n+1)/2$$

Impro_endairA verifies one digital signature at the first intermediate, one signature at the second intermediate node. Two signatures from the third intermediate node onwards If the source is n hop distance from the destination, the total number of signature verifications done in whole path from source to destination is:

$$1 + 1 + 2 + 2 + \ldots + 2 + 2 + n = 2 + 2(n-3) + n = n + 2(n-2)$$

The Computational complexity of endairA is $O(n^2)$ and Impro_endairA is $O(n)$.As the number of computations decreases the power consumption of a device also decreases. So, Impro_endairA consumes less power compare to *endairA*.

3.2 Defensive Capability of Impro_endairA

Consider a MANET contains *S, B, C, D, F, T* nodes; the route request is traveled from source S to Destination *T* through *B, C, D, F* nodes. During the Route reply propagation, node *C* can perform the malicious actions. These malicious actions are taken care by Impro_endairA.

Node *C* sends the following route reply message to node *B* after adding extra signature. At node *B* route reply is dropped, because the number of signatures is greater than the number of nodes in the node list.

(rrep, S, T, (B,C,D,F),(sigT;sigF;sigD;sigC;sigC)) (1)

Node *C* sends the following route reply message to node B after deleting the node *D*'s signature. At node *B*, while checking the two hop neighbor signatures, *B* verifies *D*'s signature which is not successful so reply dropped at node *B*.

(rrep, S, T, (B,C,D,F),(sigT;sigF;sigC)) (2)

Node *C* sends the following route reply message to node B without attaching its signature. At node *B*, while checking the two hop neighbor signatures. *B* verifies *D*'s signature which is not successful so reply dropped at node *B*.

(rrep, S, T, (B,C,D,F),(sigT;sigF;sigD)) (3)

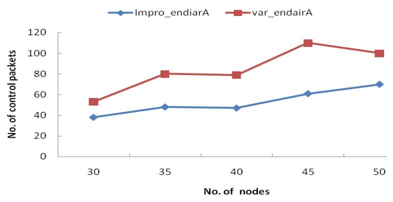

Fig. 2. Number of nodes Vs Number of control packets

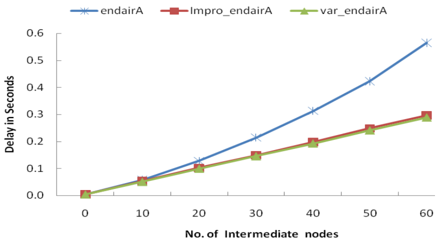

Fig. 3. Number of Intermediate nodes Vs Delay

4 Results and Discussion

We have implemented *endairA*, Variant of *endairA* and Impro_endairA in GlomoSim. In this simulation 50 mobile nodes are placed in a rectangular field of 1500m×1000 m area with transmission range of a node 376.782m. Random waypoint mobility model is used. Traffic sources are constant-bit-rate with 512 bytes packet. Fig 2 showing the graph between the number of control packets vs number of nodes. Impro_endairA reduced the number of control packets in the network compare to variant of *endairA*. In Impro_endairA the malicious route reply packets will be dropped at next immediate legitimate neighbor but where as in variant of *endairA* the malicious route reply will be dropped at source node.

Fig 3 shows the graph between number of intermediate nodes Vs end-to-end Delay. The end-to-end delay in *endairA* is increasing drastically as number of intermediate nodes is increasing because each intermediate node verifies all the signatures in the route reply packet. An Intermediate node in the Impro_endairA verifies at most two signatures in the route reply so the end-to-end delay is increasing linearly.

5 Conclusion and Future Work

In this paper we proposed impro_endairA. Proposed Impro_endairA is efficient compared to *endairA* in terms of the computational complexity and power. We have shown how Impro_endairA mitigate the attack on variant of *endairA*. Simulations have shown that the Impro_endairA outperforms variant of *endairA* and *endairA*. The attacks which are possible on *endairA* are still possible on Impro_endairA.

We need to do thorough simulations with different parameters to understand the performance of Impro_endairA.

References

1. Abidin, A.F.A., et al.: An Analysis on Endaira. International Journal on Computer Science and Engineering 02(03), 437–442 (2010)
2. Perkins, C., Bhagwat, P.: Highly DynamicDestination-Sequenced Distance Vector Routing (DSDV) for Mobile Computers. In: ACM SIGCOMM, pp. 234–244 (1994)
3. Johnson, D.B., Maltz, D.A., Broch, J.: DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, `http://www.monarch.cs.cmu.edu/`
4. Djenouri, D., Bouamama, M.: Black-hole-resistant ENADAIRA based routing protocol for Mobile Ad hoc Networks. Int. Journal on Security and Networks 4(4) (2009)
5. Djenouri, D., Badache, N.: A novel approach for selfish nodes detection in manets: proposal and petrinets based modeling. In: The 8th IEEE International Conference on Telecommunications (ConTel 2005), Zagreb, Croatia, pp. 569–574 (2005)
6. Gergely, A., Buttyan, L., Vajda, I.: Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. IEEE Transaction on Mobile Computing 5(11) (November 2006)
7. Nguyen, H.L., Nguyen, U.T.: A study of different types of attacks on multicast in mobile ad hoc networks. Ad. Hoc. Networks 6, 32–46 (2008), `http://www.sciencedirect.com`
8. Kumar, M.J., Gupta, K.D.: Secure Routing Protocols in Ad Hoc Networks: A Review. In: Special Issue of IJCCT, 2010 for International Conference (ICCT 2010), December 3- 5, vol. 2(2,3,4) (2010)
9. Fanaei, M., Fanian, A., Berenjkoub, M.: Prevention of Tunneling Attack in endairA. In: Sarbazi-Azad, H., Parhami, B., Miremadi, S.-G., Hessabi, S. (eds.) CSICC 2008. CCIS, vol. 6, pp. 994–999. Springer, Heidelberg (2008)
10. Buttyan, L., Hubaux, J.P.: Security and cooperation in wireless networks. Cambidge University Press (2008)
11. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, pp. 255–265 (2000)
12. Li, W., Joshi, A.: Security Issues in Mobile Ad Hoc Networks- A Survey (2006)
13. Hu, Y.C., Perrig, A., Johnson, D.B.: Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. In: Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom 2002), Atlanta, Georgia, pp. 12–23 (September 2002)