International Journal of Trend in Research and Development, Volume 2(5), ISSN 2394-9333
www.ijtrd.com

Randomized Multipath Routing [RMR] for Secure Data Exchange in Ad Hoc Wireless Networks

H.Santhi[1], Dr. N.Jaisankar[2]
[1]Assistant Professor (Senior), [2]Professor,
[1,2]School of Computing Science and Engineering, VIT University, Vellore, India.

Abstract: Ad hoc wireless network is a collection of nodes that is connected through a wireless medium forming a rapidly changing network topologies, ad hoc wireless network is a decentralized type of network. This makes them vulnerable to a variety of attacks which affects the reliability of data transmission within the network. Attacks on ad hoc wireless networks disrupt the overall performance and reliability of network. For example an adversary node can selectively choose a path in the network and make it a compromise node or jam all the nodes in the network. In order to provide a secured communication in an ad hoc network environment we propose a randomized multipath routing algorithm. In randomized multipart routing algorithm [RMR] multiple paths are computed in a random manner, each time an information packet needs to be sent, such that the set of routes taken by various shares of packets keeps on changing from time to time. As a result, a large number of routes can be potentially generated for each source and destination and also perform encryption technique to provide high level of security.

Keyword: Randomized Multipath Routing, Ad hoc Wireless Networks, Secure routing protocol, Reliability, Attacks.

I. INTRODUCTION

Multipath routing is the routing technique [1, 2] of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other. Other than this it also works with the overlapping of the nodes. Multi-path routing achieves load balancing [16] and is more resilient to route failures. Performance evaluations of protocols showed that they achieve lower routing overhead, lower end-to-end delay and alleviate congestion in comparison with single path routing protocols. However, a quantitative comparison of multi-path routing protocols has not yet been conducted.

In randomized multipath routing, we use a three phase approach for secure information delivery in ad hoc wireless network, in the first approach secret sharing of information is done. In the second phase randomized propagation of each information share is performed. In the third phase normal routing with minimum number of hopes from source to destination is computed. When a source node want to send a packet to the destination it first breaks the packet into P shares, according to a (P, K) threshold secret sharing algorithm [4, 15]. Each share is then transmitted into source randomly selected neighbor. That neighbor continue to forward that share, it has received to other randomly selected neighbors, and so on.

II. LITERATURE SURVEY

In [5], the author deals with the vision of nomadic computing with its ubiquitous access have stimulated much interest in the Ad Hoc Networking (ANET) technology. However, its proliferation strongly depends on the availability of security provisions, among other factors. In ANET environment any node can maliciously or selfishly disrupt and deny communication of other nodes.

In [6, 9], the authors presented and evaluated the Secure Message Transmission (SMT) protocol, which safeguards the data transmission against arbitrary malicious behaviour of other nodes. SMT is a lightweight, yet very effective, protocol that can operate solely in an end-to-end manner. It exploits the redundancy of multipath routing and adapts its operation to remain efficient and effective even in highly adverse environments.

In [7], secure data forwarding approach is developed based on feedback exchanged between the two communicating end-nodes. This feature enables effective communication even under highly adverse conditions. Moreover, features such as low-cost encoding and validation mechanisms, and partial retransmissions render the scheme efficient. By relying solely on the end-to-end security associations, SMT can secure effectively the data transmission without prior knowledge of the network trust model or the degree of trustworthiness of the intermediate nodes.

In [8,10], the author's deals with the emergence of the Ad Hoc Networking technology advocates self-organized wireless interconnection of communication devices that would either extend or operate in concert with the wired networking infrastructure or, possibly, evolve to autonomous networks. In either case, the proliferation of ANET-based applications depends on a multitude of factors,

with trustworthiness being one of the primary challenges to be met. Despite the existence of well-known security mechanisms, additional vulnerabilities and features pertinent to this new networking paradigm might render such traditional solutions inapplicable. In particular, the absence of a central authorization facility in an open and distributed communication environment is a major challenge, especially due to the need for cooperative network operation. In particular, in ANET, any node may compromise the routing protocol functionality by disrupting the route discovery process. In this paper, we present a route discovery protocol that mitigates the detrimental effects of such malicious behavior, as to provide correct connectivity information.

In [11], an efficient secure routing protocol is proposed for ad hoc networks that guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes. The protocol introduces a set of features, such as the requirement that the query verifiably arrives at the destination, the explicit binding of network and routing layer functionality, the consequent verifiable return of the query response over the reverse of the query propagation route, the acceptance of route error messages only when generated by nodes on the actual route, the query/reply identification by a dual identifier, the replay protection of the source and destination nodes and the regulation of the query propagation. The resultant protocol is capable of operating without the existence of an on-line certification authority or the complete knowledge of keys of all network nodes.

In [12], a new adaptive multipath routing algorithm is developed based on Bayesian model that defines the basic security requirements for secure communication model. It minimizes the consequences of security attacks deriving from collaborating malicious nodes in ANET.

III. IMPLEMENTATION OF PROPOSED ALGORITHM

In traditionally, counter-attack approach is used as a two-step process. First, the packet is broken into M shares using a (T, M)-threshold secret sharing mechanism [14]. The original information can be recovered from a combination of at least T shares. Second, multiple routes from the source to the destination are computed according to some multipath routing algorithm.

Three security problems exist in the above counter-attack approach [13]. First, this approach is no longer valid if the adversary can selectively compromise or jam nodes. Second, actually very few node-disjoint routes can be found when the node density is moderate and the source and destination nodes are several hops apart. Last, the set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-size black hole.

In order to overcome above problem we propose a randomized multipath routing algorithm that can overcome the above problems. In this algorithm, multiple paths are computed in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. As a result, a large number of routes can be potentially generated for each source and destination and also perform encryption technique to provide high level security. The advantage of this algorithm is adversary node has to compromise or jam all possible routes from the source to the destination, which is practically not possible. Because routes are now randomly generated, they may no longer be node-disjoint. Using the encryption technique [7] it is impossible to hack the threshold value so that adversaries cannot acquire the packets.

The figure -1 shows, the user sending data to the server, splitting the data into shares, encryption in server and how packets take the various paths in routing using randomized multipath algorithm and reaching the destination.

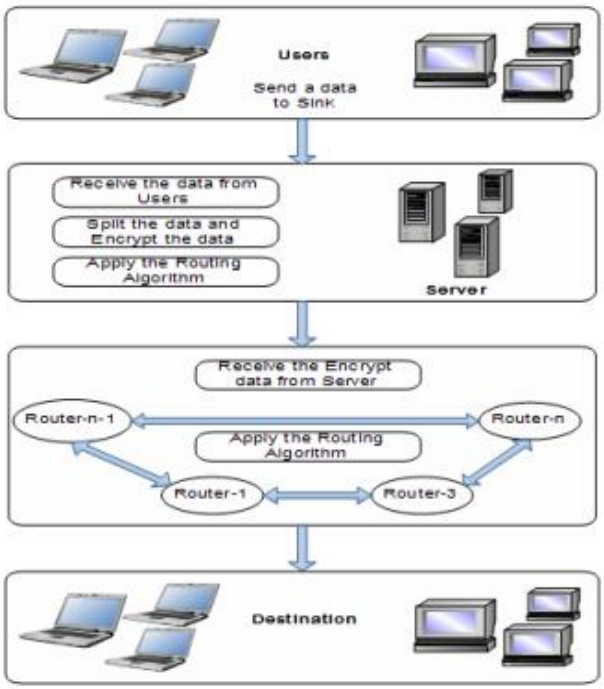

Figure 1: Proposed System Architecture

IV. DETAILED DESCRIPTION OF THE PROPOSED SYSTEM

The figure.2 shows the complete process of the proposed system. The data's are divided into shares, encrypted and assigned a TTL value .The source randomly selects the first router to send the first share and then routers dynamically select the neighbour according to the destination. The data's are decrypted in destination and reconstructed according to the TTL value.

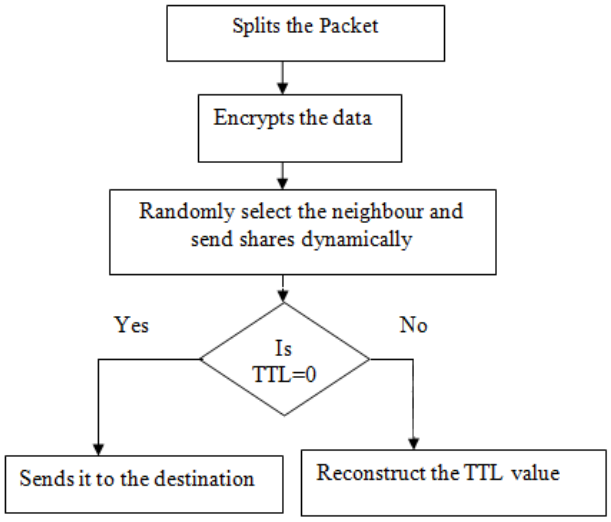

Figure.2 Completer Process of Counter Attack

It first breaks the packet into M shares, according to a (T, M)-threshold. Each share is then transmitted to some randomly selected neighbor. In each share, there is a TTL field, whose initial value is set by this module to control the total number of random relays. It automatically finds the number of destinations. Sender can select the one destination using this module.

Router will continue to relay the share it has received to other randomly selected neighbors. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last router to receive this share begins to route it toward the destination. The effect of route depressiveness on bypassing black holes. This module only collects the data from routers. Then In each share, there is a TTL field, whose initial value is set by the server to control the total number of random relays. Once the Destination collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares.

CONCLUSION

In this paper, we have discussed the problem of exchanging the packets in a secured manner. We have developed a randomized multipath routing algorithm to provide additional security levels against adversaries attempting to acquire these packets. Ad hoc network require a high level security, our current work is based on the assumption that there is only a small number of black holes in the ad hoc network. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of nodes that are several hops away from the sink to form clusters of black holes around the sink.

References

[1] D.B. Johnson, D.A. Maltz, and J. Broch, (2001) "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," *Ad Hoc Networking, C.E. Perkins, ed.,* pp.139-172.

[2] S.J. Lee and M. Gerla, (2001) "Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks," Proc. *IEEE Int'l Conf. Comm. (ICC)*, pp. 3201-3205.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, (2002) "A Survey on Sensor Networks," *IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.*

[4] C.L. Barrett, S.J. Eidenbenz, L. Kroc, M. Marathe, and J.P. Smith, (2003) "Parametric Probabilistic Sensor Network Routing," Proc. ACM *Int'l Conf. Wireless Sensor Networks and Applications (WSNA)*, pp. 122-131.

[5] Panagiotis Papadimitratos & Zygmunt J, (2003) "Secure Data Transmission in Ad Hoc Networks", *WiSe '03 Proceedings of the 2nd ACM workshop on Wireless security*.

[6] Mike Burmester & Tri Van Le, (2004) "Secure Multipath Communication in Ad hoc Networks", *International Conference on Information Technology: Coding and Computing (ITCC 2004).*

[7] M. Burmester and T.V. Le, (2004) "Secure Multipath Communication in Mobile Ad Hoc Networks*," Proc. Int'l Conf. Information Technology: Coding and Computing*, pp. 405-409.

[8] W. Lou, W. Liu, and Y. Fang, (2004) "Spread: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," Proc. *IEEE INFOCOM*, vol. 4, pp. 2404-2413.

[9] Panayiotis Kotzanikolaou, Rosa Mavropodi, Christos Douligeris, (2005) " Secure Multipath Routing for Mobile Ad Hoc Networks", *Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05).*

[10] P.C. Lee, V. Misra, and D. Rubenstein, (2005) "Distributed Algorithms for Secure Multipath

Routing," Proc. *IEEE INFOCOM*, pp. 1952-1963.

[11] X.Y. Li, K. Moaveninejad, and O. Frieder, (2005) "Regional Gossip Routing Wireless Ad Hoc Networks," ACM *J. Mobile Networks and Applications*, vol. 10, nos. 1-2, pp. 61-77.

[12] W. Lou and Y. Kwon, (2006) "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," *IEEE Trans. Vehicular Technology*, vol. 55, no. 4, pp. 1320- 1330.

[13] W. Lou, W. Liu, and Y. Zhang, (2006) "Performance Optimization Using Multipath Routing in Mobile Ad Hoc and Wireless Sensor Networks," Proc. *Combinatorial Optimization in Comm. Networks*, pp. 117-146.

[14] P.C. Lee, V. Misra, and D. Rubenstein, (2007) "Distributed Algorithms for Secure Multipath Routing in Attack-Resistant Networks," *IEEE/ ACM Trans. Networking*, vol. 15, no. 6, pp. 1490-1501.

[15] T. Claveirole, M.D. de Amorim, M. Abdalla, and Y. Viniotis, (2008) "Securing Wireless Sensor Networks Against Aggregator Compromises," IEEE *Comm. Magazine*, vol. 46, no. 4, pp. 134-141.

[16] C.Siva Ram Murthy and B.S.Manoj, (2008) "Ad Hoc Wireless Networks Architecture and Protocols", *Pearson Education*, 2nd Edition.