ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Anonymity Set Location Privacy Scheme in Manet

T.Sathish[*1], U.Muthaiah[2]
[*1,2]Department of Computer Science & Engineering, Sri Shanmugha College of Engg&Tech
Salem, Tamil Nadu, India
vptsathish@gmail.com

Abstract

In hostile environments, the adversary can launch traffic analysis against intercept able routing information embedded in routing messages and data packets. The adversaries on tracing network routes and inferring the mobility pattern of nodes during the routing of packets may pose a serious threat to covert operations. Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. The anonymous routing protocols can be applied to different network models with different mobility patterns. By means of route anonymity, adversaries cannot trace a packet flow back to its source or destination, either on the route or out of the route and no node has information about the real identities and locations of intermediate nodes in route. The various anonymous routing protocols are reviewed and performance of such protocols can be compared and evaluated using ns2 simulations of a well-known routing protocol to achieve better route anonymity.

Keywords: Adversary, Anonymousrouting, Mobile Adhoc Networks, Mobility.

Introduction

A Mobile Ad Hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. A mobile ad hoc network (MANET) is generally as a network that has many free or autonomous nodes. Due to open medium and decentralization features, MANETsis usually not desirable to constrain the membership of the nodes in the network. Security of communication in MANET is important for secure transmission of information. Absence of any central coordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network. Nodes in MANETs are susceptible to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. *However, anonymous location based-efficient routing protocol* is distinguished by its low cost and full anonymity protection for sources, destinations, and routes. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity of nodes and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. “Identity and location anonymity of sources and destinations” means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations.

The anonymous routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. The anonymous route discovery process establishes an on demand route between a source and its destination. Each hop en route is associated with a random route pseudonym. Since the forwarding of data packets in the network is based on route pseudonyms with negligible overhead, local senders and receivers need not reveal their identities in wireless transmission. The route anonymity problem to implement a untraceable routing scheme, where each route consists of a set of hops and each hop is identified by a route pseudonym. For each multi-hop route, we seek to realize relationship anonymity among the corresponding set of route pseudonyms. The route pseudonymity approach differentiates this work from earlier studies addressing identity pseudonymity (e.g., person pseudonymity, role pseudonymity, and transaction pseudonymity). The route pseudonymity approach enables location

privacy support that realizes unlink ability between a mobile node's identity and its location.

Privacy attacks to ad hoc routing protocols become an important issue as mobile ad hoc networks enter security critical domains. Location privacy attacks can be performed by tracing either route discovery messages or data packets in order to discover the message's origin or destination. It is clear that providing anonymity in adhoc networks is important as users may wish to hide the fact that they are accessing some service or communicating with another user. Another application is hiding the location of users participating in the network. Hiding nodes that participate in the network also makes it more difficult for an adversary to focus his attack as he will not be able to identify and locate the more active nodes within the network.

Literature Survey

The topology-based routing in mobile ad hoc networks in[3], attempt to utilize available location information helps making localized decisions that are essential to the network scalability and does not offers privacy protection .To overcome this problem the Anonymous Geographic routing algorithm has been introduced. It requires each node to periodically update its current location to its neighbors and possibly remote servers. Using methodology in Anonymous neighbor table, Anonymous greedy forwarding, Anonymous Location Service areused to guarantee protection while location information is used to maintain the efficiency of geographic routing. Greedy forwarding has a satisfactory delivery performance even in a modest-density network. Increases 23% network density, location information is used to maintain the efficiency of geography routing and achieve both location and identity.

The individual nodes cooperate by forwarding packets for each other to allow nodes to communicate beyond direct wireless transmission range. Prior research in ad hoc networking has generally studied the routing problem in a non-adversarial setting, assuming a trusted environment. The secureon-demand ad hoc network routing protocol has been proposed in [4]. There are two contributions first, a model for the types of attacks possible in such a system, and described several new attacks on ad hoc network routing protocols. Second, the design and performance evaluation of a new on-demand secure ad hoc network routing protocol, called Ariadne has been presented. Ariadne provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetriccryptographic operations. The security mechanisms are designed and highly efficient. Ariadne actually performs better41.7% lower packet overhead than for optimizedDSR.

Aad et al, offered the basic idea for the wired Internet, has been used to "mix" mail servers that randomly delay mail forwarding, thus reducing the correlation between incoming and outgoing mails and hiding who is communicating with whom. On a smaller scale, packets contain all the necessary information to be forwarded along the path from the source to the destination. Onion routing is at the basis of several enhanced techniques used for anonymous communications in ad hoc networks. The proposed ANODRprotocol [5], is a quite efficient approach for untraceable routing based on link pseudonyms.ANODR relies on the novel idea of broadcast with trapdoor information. ANODR provides excellent performance to thwart local attackers, but it does not diversify packet routes and retransmission the packet. The result combination is a constantly changing/unrecognizable packet (header and payload), being routed on a multicast tree to reach a given anonymity set whilereducing41.1% the transmission costs and secures the packet.

In the mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. The author introduced an Anonymous Location-Aided Routing in MANETs (ALARM)[6], which demonstrates the feasibility of obtaining, at the same time, both strong privacy and strong security properties. ALARMrelies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The frame work with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes.

The MANETs does not require privacy and number of MANET routing protocols ranging widely in assumptions, efficiency and functionality. MANET routing focused on security issues, less attention has been devoted toprivacy. The protocol PRISM: Privacy-friendly Routing in Suspicious MANETs in [7] is an anonymous location-based on-demand routing protocol based on three main building blocks: (1) the well-known AODVrouting protocol, (2) any secure group signature scheme (3) location information. The main problem is topology information unsalable. (PRISM) with strong privacy and security features. PRISM is resistant to node tracking by both outsider and insider adversaries. The results ofPRISM with an alternative location-centric link-state approachshowed that PRISM generally

achieves better performance under reasonable communication assumptions.

The Mobility model for cellular and adhoc wireless network with various mobility patterns affect the performance of different network protocols in different ways. A flexible mobility framework which allows us to model different applications and network scenarios and to identify the impact of mobility on different scenarios. To overcome the problem with the existing work, the mobility framework called Reference Point Group Mobility (RPGM) model has been developed in [8]. The center's motion defines the entire group's motion behavior, including location, speed, direction, acceleration, etc. The reference point scheme allows independent random motion behavior for each node, in addition to the group motion. The Random model generates higher rate of change in connectivity than group model. The results is not sufficient to test it with Random walk type mobility models since the motion pattern can interact in a generally positive also added 13.1% mobility and improves the performance.

The anonymity and security properties of the routing protocol and notice that previous research works provided only the Weak Location Privacy and Route Anonymity, and are vulnerable to specific attacks. The Anonymous Secure Routing (ASR) protocol in [9] can provide additional properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy. The drawbacks identified are weak route link and link break occurred in data transmission helps in improving the efficiency and repairing broken routes locally but, without compromising anonymity and security.

The privacy of ad hoc networks by the using broadcast or multicast scheme for receiver privacy are not sufficient. Geographic or position-based routing algorithms for ad hoc networks have been widely studied in addition to node ID, extra information, such as the positions of the nodes, could be used for making routing decisions. Ad hoc on-demand position-based private routing algorithm called A02P, is proposed in [10], for communication anonymity. Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information. The route failure and high node density are concerned and achieved48.6% communication privacy greatly in ad hoc network also, focused privacy evaluation, security issue and mitigation techniques.

The Privacy enhanced technique and providing security for MANETs has been a challenging task. An anonymous on demand routing protocol for MANETs considered to be secure against both nodes that actively participate in the network and a passive global adversary that monitors all network traffic.Anonymous routing protocol in [11], enables private communications between users while making it harder for adversaries to focus their attacks. The dataforwarding message is not in secure manner in the proposed method, which is easily identified by the viewers.

The Geographic information is required for LBSs and (MANETs) as an effective solution for extending infrastructurebased wireless network communications /self-constructing when fixed infrastructures are not available.Wu&Liu [12]introduced Zone-based anonymous positioning routing protocol, preserves destination anonymity through the use of anonymity zone, under which a destination is collocated with a number of other nodes. An anonymousgeo-routing protocol that adopts fuzzy positions to create anonymity zone for destination anonymity. Nodes residing in the anonymous zone form the anonymity set, which protects the real destination. The proposed method failed to detect the low density and low protection.It significantly increases packet delivery ratio and improves the routing performance.

The Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities / routes from outside observers in order to provide anonymity protection. The Existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic either generates high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To offer high anonymity protection at a low cost, the authorintroduced an Anonymous Location-based Efficient Routing protocol (ALERT) [13], dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen the source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. The proposed scheme does not consider the active internal attackers.

Result and Discussion

The cumulated actual participating nodes in ALERT, GPSR[14], ALARM, and AO2P, with 100 and200 nodes moving at a speed of 2 m/s,

ISSN: 2277-9655
Impact Factor: 1.852

respectively. Since ALARM and AO2P[15], are similar to GPSR in the routing scheme and thus have similar number of actual participating nodes, used GPSR to also represent ALARM and AO2P in discussing the performance difference between them and ALERT. ALERT generates many more actual participating nodes since it produces many different routes between each S-D pair. The number of actual participating nodes is up to 30 in the 100 nodes case and is up to 45 in the 200 nodes case. The results are close to the analytical results of the number of possible participating nodes. In ALERT, more nodes in the network produce more participating nodes because each routing involves more new random forwarders, which is a key property of ALERT to provide routing anonymity

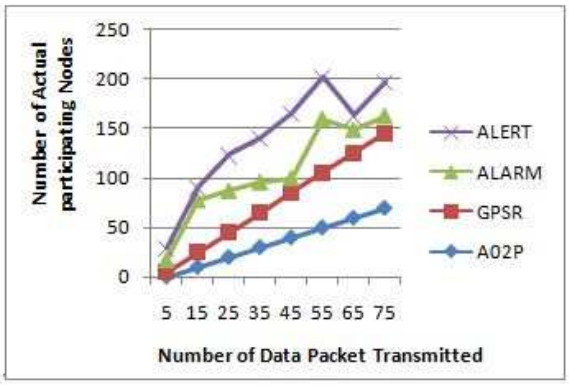

Fig.3.1 Different Number of Packet Transmitted

On the contrary, Figure.3.1 shows that GPSR only has slight increase in the number of participating nodes because it always takes the shortest path by greedy routing. The number of actual participating nodes after the transmission of 20 packets versus the number of nodes in the network. The number of actual participating nodes in GPSR is steady with a marginal increase. This is due to the reason that the increased node density provides shorter routes. Also, ALERT generates dramatically more participating nodes than GPSR. GPSR has only 2-3 nodes while ALERT has 13-20. More participating nodes lead to more randomized routes that is difficult to detect or intercept. Therefore, the results illustrate higher route anonymity property of ALERT.

On the contrary, the shortest routing paths in ALARM, AO2P, and GPSR follow the same greedy routing principle, which are easy to be identified by the adversaries and reduce the traffic analysis. The number of nodes that have moved out of the destination zone increases. Even though ALERT generates more routing hops than AO2P and ALARM. ALERT generates a slightly longer latency than GPSR.ALERT has slightly higher hops per packet than ALARM, AO2P, and AO2Pand GPSR.

Conclusion

Anonymous routing schemes in MANETs have been studied in recent years. By the different usage of topological information, they can be classified into on-demand or reactive routing methods and proactive routing methods. Since topology routing does not need the location information of nodes, and it is not essential to provide anonymity protection. Therefore, an anonymous communication protocol that can provide intractability to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity.

References

[1] J. Kong and X. Hong, "Anodr: anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Manets '03: Proceedings of the 4th ACM international symposium on Mobile adhocnetworking& computing, New York, NY, USA, 2003, pp. 291–302.

[2] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper." in ICNP. IEEE, 2007, pp. 314–323.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic AdHocRouting for Preserving Location Privacy, "Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW),2005,pp. 646–651.

[4] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[5] Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, pp.1-10, 2006.

[6] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l

ISSN: 2277-9655
Impact Factor: 1.852

Conf. Network Protocols (ICNP), 2007, pp. 304-313.

[7] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008, pp.258-267.

[8] J. Kong and X. Hong, "Anodr: anonymous on demand routing for mobile ad-hoc networks," MobiHoc, pp.291-302, 2007.

[9] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003,pp.102–108.

[10] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans.Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309,2008.

[11] Stefaanseyes.G and Bart preneel.L "Arm: Anonymous routing Protocol for Mobile Ad-Hoc Networks," IEEE J. Selected Areas inComm., vol. 25, no. 1, pp. 192-203, 2007.

[12] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans.Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309,2008.

[13] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), pp.1079-1093, 2013

[14] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, pp. 243-254, Aug. 2000.

[15] X. Wu and B. Bhargava, "Ao2p: ad hoc on-demand position based private routing protocol," IEEE Transactions on Mobile Computing, pp. 335-348, 2005.