International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

A Survey on ALERT: An Anonymous Location-Base Efficient Routing Protocol

Nayyar Ansari[1], Premala Patil[2]
[1] Student, ECE Department, Guru Nanak Dev Engineering College Bidar, Karnataka, India
[2] Assistant Professor, ECE Department, Guru Nanak Dev Engineering College Bidar, Karnataka, India

Abstract: **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. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic either generate 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, I propose an Anonymous Location-based Efficient Routing proTocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen 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. In this paper I briefly presents the survey conducted in this regard.**

Key Words: **Mobile ad hoc networks, anonymity, routing protocol, geographical routing**

1. INTRODUCTION:

Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, an entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage. 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 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. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination [1], it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [2], [3], [4], [5], [6] and redundant traffic [7], [8], [9], [10], [11], [12], [13]. Most of the current 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. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM [5] cannot protect the location anonymity of source and destination, SDDR [14] cannot provide route anonymity, and ZAP [13] only focuses on destination anonymity. Many anonymity routing algorithms [3], [4], [13], [5], [6], [11], [10] are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) [15]) that greedily forwards a packet to the node closest to the destination. However, the protocol's strict relay node selection makes it easy to reveal the source and destination and to analyze traffic. On the other hand, limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. Further, the recent increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations. In order to provide

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing proTocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR [15] algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks [16] and timing attacks [16].

In summary, the contribution of this work includes: 1. Anonymous routing. ALERT provides route anonymity, identity, and location anonymity of source and destination. 2. Low cost. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection. 3. Resilience to intersection attacks and timing attacks. ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue [16]. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair.

2. EXISTING SYSTEM:

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 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. For route anonymity, adversaries, either enroute or out of the route, cannot trace a packet flow back to its source or destination, and no node have information about the real identities and locations of intermediate nodes enroute. Also, in order to dissociate the relationship between source and destination (i.e., relationship un-observability, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

3. DISADVANTAGES OF EXISTING SYSTEM:

- The current 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.
- Many approaches cannot provide all of the aforementioned anonymity protections
- ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity
- Existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

4. ALERT:

In order to provide high anonymity protection (for sources, destination, and route) with low cost, I propose an Anonymous Location-based and Efficient Routing proTocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks. We theoretically analyzed ALERT in terms of anonymity and efficiency.

Networks and Attack Models and Assumptions ALERT can be applied to different network models with various node movement patterns such as random way point model [17] and group mobility model [18]. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message’s sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide un traceability is needed 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. The assumptions below apply to both inside and outside attackers.

1. Capabilities: By eavesdropping, the adversary nodes can analyze any routing protocol and obtain information about the communication packets in their vicinity and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

record the historical communication of nodes. They can intrude on some specific vulnerable nodes to control their behavior, e.g., with denial-of-service (DOS) attacks, which may cut the routing in existing anonymous geographic routing methods.

2. In capabilities: The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers

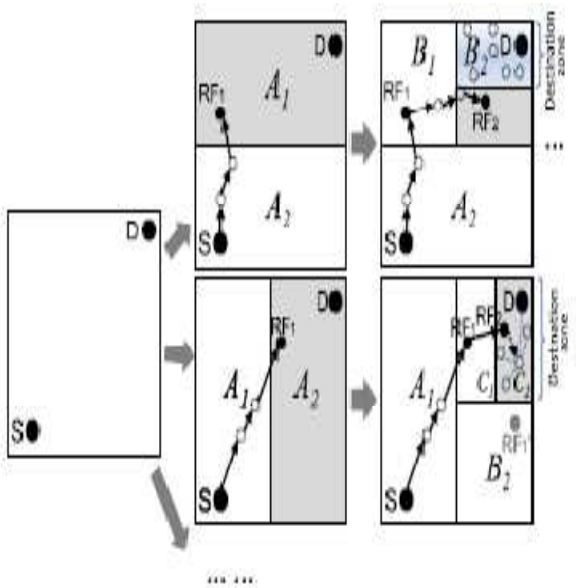

Fig1: Different Zone Partitions

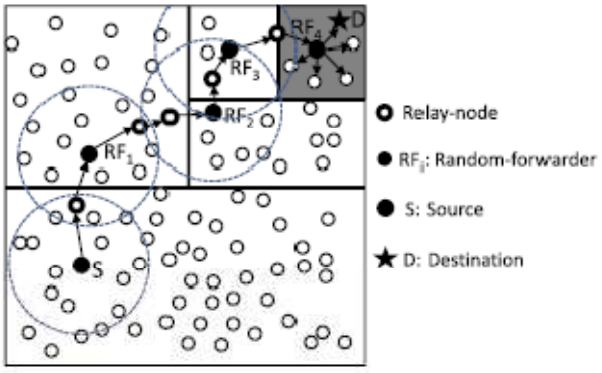

Fig2: Routing Among Zones

5. ADVANTAGES OF PROPOSED SYSTEM:

- ALERT provides route anonymity, identity, and location anonymity of source and destination
- Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
- ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair.

6. CONCLUSION AND FUTURE WORK:

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers.

It has the “notify and go” mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT’s ability to fight against timing attacks can also be analyzed.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, “Anonymity,Unlinkability,Unobservability,Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,” technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet (SAINT), 2006.

[3] Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,” Proc. Third Int’l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[4] V. Pathak, D. Yao, and L. Iftode, “Securing Location Aware Services over VANET Using Geographical Secure Path Routing,” Proc. IEEE Int’l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.

[6] K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

[7] 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.

[8] I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops,2006.

[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, “An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[10] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[11] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, “Anonymous Secure Routing in Mobile Ad-Hoc Networks,” Proc. IEEE 29th Ann. Int’l Conf. Local Computer Networks (LCN), 2004.

[12] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.
[13] 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, Oct. 2008.
[14] 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.
[15] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.
[16] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.
[17] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
[18] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
[19] Debian Administration, http://www.debian-administration.org/ users/dkg/weblog/48, 2012.
[20] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.
[21] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. 32nd Int'l Conf. Very Large Databases (VLDB), 2006.
[22] J. Li, J. Jannotti, D.S.J. De, D.S.J. De Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, 2000.
[23] Y. Xue, B. Li, and K. Nahrstedt, "A Scalable Location Management Scheme in Mobile Ad-Hoc Networks," technical report, 2001.
[24] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, 2000.
[25] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5,
pp. 557-570, 2002. [26] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, "Analyzing the Energy Consumption of Security Protocols," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED), 2003.
[27] H. Frey and I. Stojmenovic, "On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor Networks," Proc. ACM MobiCom, 2006.
[28] K.C. Lee, J. Haerri, L. Uichin, and M. Gerla, "Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios," Proc. IEEE GlobeCom Workshops, 2007.
[29] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.
[30]"KeLiu'sNS2Code,"http://www.cs.binghamton.edu/~kliu/
research/ns2code/index.html, 2012.
[31]"TheNetworkSimulator-ns-2," http://www.isi.edu/nsnam/ns, 2012.
[32] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.
[33] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.
[34] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.
[35] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient
Distance Vector Routing for Mobile Wireless Ad
Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.
[36] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.
[37] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.