T.Hari Shankar *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 79-85 **ISSN: 2321-8363**

GPSR GEOGRAPHICAL ROUTING PROTOCOL USING MANET

Mr.T.Hari Shankar[1], Mr.S.Dilip Kumar[2]

[1] *PG Student,* [2]*Assistant Professor, Department of Computer Science and Engineering,*

PRIST University, Trichy District, India

([1] harishankarcse@live.com)

Abstract

MANETs is self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. 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. 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. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs, its use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection and 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. It's theoretically analyzing ALERT in terms of anonymity and efficiency. Experimental results exhibit consistency with the theoretical analysis, and show that ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Many anonymity routing algorithms are based on the geographic routing protocol (e.g. Greedy Perimeter Stateless Routing (GPSR)) 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 the traffic.

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 and 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 analyse 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, 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.

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. On the other hand, limited resource is an inherent problem in MANETs, in which each node labours under an energy constraint. MANET's 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 order to provide 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 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.

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. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source-destination pair.

4. Extensive simulations:

We conducted comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols.

2 LITERATURE SURVEY

2.1 Statement of project

2.1.1 An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks:

Due to the infrastructure-less, dynamic and broadcast nature of radio transmissions, communications in mobile ad hoc networks (MANETs) are susceptible to malicious traffic analysis. After traffic analysis, an attacker determines a target node and conducts an intensive attack against it, called target-oriented attack. The traffic analysis and the target-oriented attacks are known as quite severe problems in MANETs, including position-based routing protocols, with respect to the degradation of both throughput and security of the routing. Also position information of routing nodes is very sensitive data in MANETs where even nodes not knowing either other establish a network temporarily. Therefore we propose a new position-based routing protocol which keeps routing nodes anonymous, thereby preventing possible traffic analysis. To this end, a time variant temporary identifier temp ID is computed from time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and temp ID is used for establishing the route for sending data: a receiver hand

shake scheme is designed for determining the next hop on-demand with use of the temp ID. We evaluate the level of anonymity and performance of our scheme. The analysis shows that the proposed scheme ensures the anonymity of both route and nodes and the robustness against the target-oriented attack and several others. Also our scheme is applicable to networks with any density of nodes.

2.1.2 Anonymzing Geographic Ad Hoc Routing for Preserving Location Privacy:

Due to the utilization of location information, geographic ad hoc routing present's superiority in scalability compared with traditional topology-based routing in mobile ad hoc networks. However, the consequent solicitation for location presence incurs severe concerns of location privacy, which has not been properly studied.

In this paper, This attempt to preserve location privacy based on the idea of dissociating user's location information with its identity. We propose an anonymous geographic routing algorithm which includes three components to avoid the explicit exposure of identity and location in communication without compromising the efficiency guaranteed by geographic routing.

2.1.3 Anonymous Communications in Mobile Ad Hoc Networks:

Due to the broadcast nature of radio transmissions, communications in mobile ad hoc networks (MANETs) are more susceptible to malicious traffic analysis. In this paper we propose a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. Based on a new cryptographic concept called pairing, we first propose an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities. Then utilizing the secret pairwise link identifiers and keys established between neighbors during the neighborhood authentication process, MASK fulfills the routing and packet forwarding tasks nicely without disclosing the identities of participating nodes under a rather strong adversarial model. MASK provides the desirable sender and receiver anonymity, as well as the relationship anonymity of the sender and receiver. It is also resistant to a wide range of adversarial attacks. Moreover, MASK preserves the routing efficiency in contrast to previous proposals. Detailed anonymity analysis and simulation studies are carried out to validate and justify the effectiveness of MASK.

2.1.4 On delivery guarantees of face and combined greedy-face routing in ad hoc and sensor networks:

Wireless multihop ad hoc networks are defined by wireless network nodes communicating without using a fixed network infrastructure. Due to limited communication ranges sending a message from source to destination often requires collaborating intermediate forwarding nodes. Limited battery capacity and limited overall communication bandwidth mandates that message forwarding which is also referred as routing has to be performed in a resource efficient manner. Geographic routing forms a specific class of routing protocols which requires that each network node is able to determine its coordinates by means of a location system like GPS or relative positioning based on signal strength estimation. Each routing step requires knowledge about the location of the message's final destination. When the destination location is not known in advance, it has to be requested by using a location service which provides a mapping from node addresses to their physical locations.

The majority of geographic routing protocols enable message forwarding in a localized manner, i.e. deciding the next routing hop is based solely on a constant amount of information stored in the message, and the location of the current node, its neighbors, and the message's final destination. Localized routing protocols can further be classified regarding their delivery guarantees. Guaranteed delivery refers to the ability of successfully forwarding a message from source to Destination. The definition requires that source and destination are connected by at least one path in the network and that we have an idealized MAC layer where messages are not lost during any forwarding step.

3 EXISTING SYSTEM

3.1 Overview of Existing System:

Existing anonymity routing protocols in MANETs can be mainly classified into two categories:

1. Hop-by-hop encryption and

2. Redundant traffic.

- 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 a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in network operations.
- 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 therefore mentioned anonymity protections.

3.2 Disadvantage:

- 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.

4 PROPOSED SYSTEM

4.1 Overview of Proposed system:

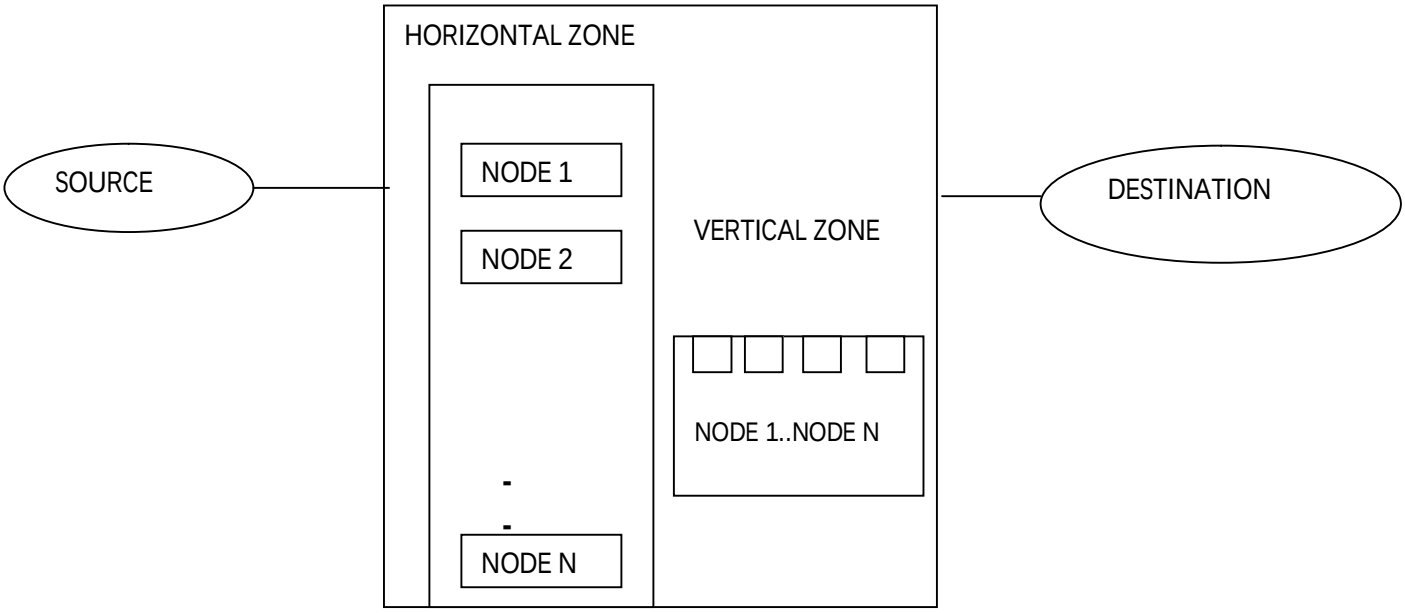
In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing proTocol (ALERT).

- 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 algorithm to send the data to the relay node.
- 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.
- We theoretically analyzed ALERT in terms of anonymity and efficiency.

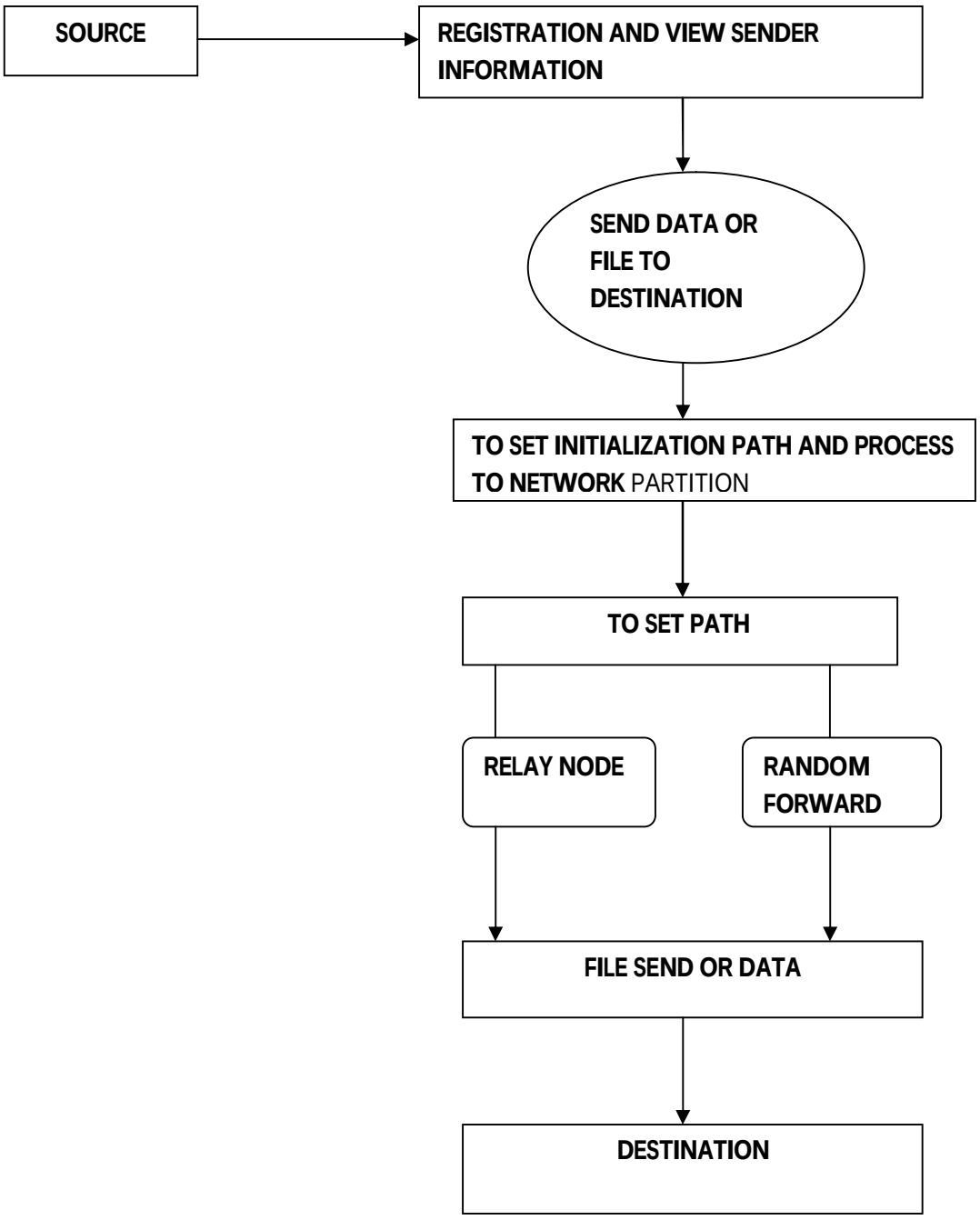
4.2 Advantage:

- 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 nonfixed routing paths for a source destination pair.

5 SYSTEM ARCHITECTURE



6 DATAFLOW DIAGRAM



CONCLUSION

In this project, I proposed 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.In the future work, To examine the performance of more comprehensive solutions by using to provide high anonymity protection and dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes.A data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source and also resilient to intersection attacks and timing attacks.To 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. The conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols.

REFERENCES

- 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.
- Sk. Md. M. Rahman, M. Mambo, A. Inomata, and E. Okamoto. An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks. In Proc. of SAINT, 2006.
- Z. Zhi and Y. K. Choong. Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy. In Proc. of ICDCSW, 2005.
- V. Pathak, D. Yao, and L. Iftode. Securing location aware services over VANET using geographical secure path routing. In Proc. Of ICVES, 2008.
- K. El Defrawy and G. Tsudik. Alarm: Anonymous location-aided routing in suspicious Manets. In Proc. of ICNP, 2007.

