www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13462-13464

Anonymous Routing Protocols in MANETs - A Survey

Sethulekshmi C G, Manoj Kumar G

[1]PG Scholar, Computer Science and Engineering,
LBS Institute of Technology for Women,
Poojappura, Trivandrum
Sethu.lekshmi1@gmail.com

[2] Associate Professor, Computer Science and Engineering,
LBS Institute of Technology for Women,
Poojappura, Trivandrum
Manojkumar_gg@hotmail.com

Abstract: ***Mobile Ad-hoc network is a collection of nodes that dynamically connected together to form a network without using any fixed infrastructure. Mobile nodes are connected by wireless links to form an arbitrary topology. As it is infrastructure less network, the information or data packets are send between the nodes with the help of radio signals and each node act as routers. MANET aimed is to provide communication capabilities to areas where limited or no predetermined communication infrastructures exist. MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. For security issue one solution is to use anonymous routing in the network that cannot be identified by any other nodes or attacker or observer. High Security and privacy in ad-hoc networks has been a major issue, while it comes in the field of defense and other such sensitive communications. Most of the communication system provides security in routing and data content. Anonymous communications should focus on anonymity in identity, location and route of the participating nodes. Anonymous communication between the Manet nodes are challenging as the nodes are free to move anywhere. No centralized node is there to monitor or to control the other nodes. Here the chance of attack from malicious nodes is high. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers.***

Keywords: MANET, GPSR, Routing Algorithm,ALERT

1. Introduction

Wireless networks can be mainly categorized as, infrastructure wireless networks and infrastructure-less wireless networks. MANET is a type of infrastructure-less wireless network which is dynamic in nature and nodes are mobile. A routing protocol for MANETs is a convention that governs all the nodes within the network to decide how to find a route to the destination in a Mobile Ad hoc Network. Routing between two nodes in an ad-hoc network is not an easy task because of the mobile nature of nodes. Moreover, a node can quit or switch the network suddenly. Mobile ad-hoc networks require anonymous communications in order to prevent wireless attacks; and to protect new assets of information such as nodes locations, motion patterns, network topology and traffic patterns in addition to conventional identity and message privacy. Anonymity and location privacy guarantees for the deployed ad hoc networks are critical in military and real time communication systems, otherwise the entire mission may be compromised. This poses challenging constraints on MANET routing and data forwarding. To address the new challenges, several anonymous routing schemes have been proposed.

Every mobile node in MANET plays a router role whereas transmission knowledge over the network. Anonymous means to hide or to be unknown to outside world. Anonymous communication methods, try to prevent traffic analysis attacks by hiding nodes' identities from outside observers. Anonymity is an important part of the overall solution for truly secure Mobile Ad-hoc Networks (MANET), especially in certain privacy-vital environments. In MANET it is very important to provide anonymity to location, identity and routes. Early routing protocols were based on either hop-by-hop encryption or redundant traffic, but these results into high cost, high traffic and low anonymity.

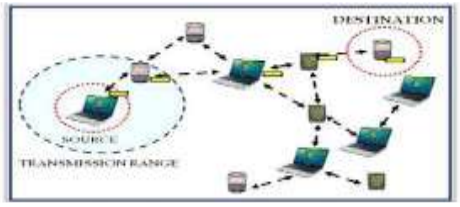

Fig: Mobile Adhoc Netorks

An anonymous communication method in MANETS is mostly classified into three type's reactive methods (on-demand), proactive methods and hybrid routing method.

2. Characteristics of MANETs

2.1 ***Dynamic topologies:*** The nodes in the network moving with different speeds, which results in the variations in the structure of the network, i.e. the nodes can join or leave the network at anytime so the topology of the network is dynamic in nature.

2.2 ***Energy constrained operations:*** The devices in the modern electronic world completely rely on batteries. The design of the network is to be optimized to conserve the

energy consumed by the mobiles.

2.3 ***Limited bandwidth:*** The bandwidth of the wireless network is very much limited and the networks are to be optimized to perform with the maximum efficiency within the limited bandwidth.

2.4 ***Multi-hop routing:*** When a node tries to send a packet to other nodes which is out of its communication range, then the packets are forwarded through one or more intermediate nodes.

2.5 ***Security threats:*** When compared to wired means of communication, wireless means of communication is more affected for security. The security of the MANET is to be optimized so that the information transferred is secured.

3. Advantages of MANETs

3.1 Infrastructure less and lower cost

3.2 Mobility

3.3 Fast Installation

3.4 Fault Tolerance

3.5 Speed

4. Disadvantages of MANETs

4.1 Limited resources and physical security.

4.2 Lack of authorization facilities.

4.3 Volatile new topology make it hard to detect malicious nodes

5. Literature Survey

Anonymous routing protocols are important 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 and destinations, as well as route anonymity. Identity and location anonymity of sources and destinations means that it is hard 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 have information about the real identities and locations of intermediate nodes en-route so, in order to dissociate the relationship between source and destination , 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.

AODV is a reactive routing protocol in which the routes are created only when they are needed. It uses routing tables. In AODV, when a source node sends packet to a destination node, it first initiates a route discovery process. In this process, the source node broadcasts a Route Request (RREQ) packet. Neighbor nodes which do not know an active route for the requested destination node forward the packet to their neighbors until an active route is found or the maximum number of hops is reached. When an intermediate node gets the active route to the requested destination node, it sends a Route Reply (RREP) packet back to source node in unicast mode. At the end source node receives the RREP packet and opens the route.

"X. Wu" proposed "A02P", which is mainly proposed for communication anonymity. In this protocol only the position of the destination is exposed in network for route discovery. To discover the routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are used for data packet delivery after a route is established. Read identifiers for source and destination nodes and forwarding nodes in end to end communication are kept private. Anonymity for destination relies on the difficulty of matching geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary.

"K.E. Defrawy and G. Tsudik" presented "ALARM" protocol, in this each node at times disseminates its hold identity to its genuine neighbors and continually collects all other nodes' identities. So the nodes can assemble a secure map of other nodes for geological routing. ALARM cannot secure the location anonymity of source and destination, it also cannot offer route anonymity, and but only focuses on destination anonymity.

In Privacy-friendly Routing in Suspicious MANETs, K.E. Defrawy and G. Tsudik said "Mobile Ad-Hoc Networks are particularly useful and well-suited for critical scenarios, like military, law enforcement as well as emergency services and disaster recovery". When operating in hostile or suspicious environment, MANETs require communication security and privacy, especially, in underlying routing protocols. This paper mainly focuses on privacy aspects of mobility. Unlike most networks, where communication is based on long-term identities, we argue that the location centric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries.

6. DISADVANTAGES OF EXISTING SYSTEM

6.1 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.

6.2 Many approaches cannot provide all of the aforementioned anonymity protections

6.3 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.

7. Proposed Enhancements

Existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic, which either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. To offer high anonymity protection at a low cost, we propose an Anonymous Location-

based Efficient Routing protocol (ALERT). ALERT dynamically partitions a net-work field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. 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.

8. Alert Routing Algorithm

8.1 First ALERT partitions given network area into two zones as horizontally (or vertically).

8.2 Then again split every partitions into two zones as vertically (or horizontally). This process is known as hierarchical zone partition.

8.3 After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node, in this way. ALERT provide dynamically creating an unpredictable routing path.

9. Advantages of Proposed system

9.1 ALERT provides route anonymity, identity, and location anonymity of source and destination.

9.2 Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

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

CONCLUSION

Prior 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 also has a capability for anonymity protection of source and destination by hiding the data initiator/receiver. 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 and timing attacks.

References

[1] 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] Kavita Taneja, R.B. Patel "An Overveiw of Mobile Ad hoc Networks: Challenges and Future." [

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

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

[5] 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.

[6] 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.

[7] 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.

[8] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.

[9] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[10] 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.