ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

COMPARISION ON VARIOUS ANONYMOUS ROUTING PROTOCOLS IN MANET

S.Indhurekha[1], AP/CSE
Vignesh Rajkumar[2], II year CSE
Tamilselvan.C[3], II year CSE
SNS College of Technology, Coimbatore

Abstract: *-Mobile adhoc network is a network (MANET) which consists of set of mobile nodes communicating with each other without any base station. The main feature and benefit of a mobile ad-hoc network is it has no fixed infrastructure, and having changing topology, which is smooth to malicious traffic analysis. Adversaries, if allowed to trace network routes and then the secret operations may be affected. So anonymity is needed, to avoid all these attacks. Providing anonymity to the routes, source and destination is a one of the important factor. This paper poses challenging constraints on anonymous MANET routing and data security. To tackle the new challenges, some anonymous routing schemes have been proposed newly. And the result shows that some of the anonymous routing protocol satisfies the requirement of network in different manner.*

INTRODUCTION

MANETs or Mobile Ad hoc Networks is an promising, exhilarating and important technology in these days because of the fast growth of wireless mobile devices. A MANET is a set of mobile nodes and these nodes cooperate by forwarding packets to each other. And they allow them to communicate beyond their range of direct wireless transmission. A MANET consists of mobile nodes that can move freely in an unlock environment. Communication between the nodes in a Mobile Adhoc network usually takes place with the help of other intermediate nodes to establish communication channels. In such an open environment, when the mobile nodes communicate with each other malicious intermediate nodes might be a threat to the security. The security problems from the Wired network world is of very little when compared with the security problems in Wireless Mobile Adhoc networks, because of some unique differences between the two Networks. MANETS are vulnerable to attacks than wired networks. Because it is an Open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense are some of the main vulnerabilities faced in MANETS.

The main applications of MANETs are military exercises, disaster relief, and mine site operation etc. These applications possibly will benefit from adhoc networking, but secure and reliable communication is the primary and necessary requirement for these applications. The primary anxiety is became security in order to provide a secure and protected communication between mobile nodes in an open hostile environment. First, we need to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

identify the new anonymity requirements for mobile wireless networks. Existing anonymity research has to make new underlying assumptions when it considers the case of mobile nodes.

Thus, those intended for fixed networks do not sustain mobile environment. Therefore, design principles of new countermeasures have to be studied. A hybrid approach of identity-free routing and on-demand routing can meet the requisites of a wireless network. This hybrid routing scheme is called ANonymous On Demand Routing (ANODR) [4]. There are various other anonymous routing protocols being used to attain anonymity. Anonymous routing is becoming more relevant in the present scenario of networks as there is an increased use of wireless networks.

The aim of the study is to discuss different anonymous protocol to provide security and privacy in MANET [5]. This paper focuses on the survey of different anonymous routing protocols and is given in the following sections. Section II presents the literature survey of different anonymous routing protocols .

II.Literature Survey

Necessity of Anonymity in a MANET

Anonymity is the state of being unidentifiable and unlinkable within set of subjects. Concept of anonymity has recently attracted the attention in mobile wireless security study. In before Proactive routing schemes are used in infrastructure networks to provide anonymity protection. These are not applicable in the case of mobile ad hoc networks. Mobile nodes are traceable by methods which are impossible in infrastructure networks. In unfriendly environments, the attacker can launch traffic analysis against interceptable routing information in routing messages and data packets. This should be prevented to make sure that active attacks do not take place. Route anonymity and location privacy are the two major issues to be handled by the anonymous routing protocol.

Anonymous Protocols

The proactive routing approach and the other approach were the overriding choices in anonymous routing design. But these became impractical in wireless environment. Then came proposals like Anonymous On Demand Routing (ANODR) [4] , Anonymous Dynamic Source Routing (AnonDSR) [6] , MASK [7] , ALARM [8], DSDV, AODV [1], AASR [13] (Authenticated Anonymous secure routing protocol) to perform the anonymous routing.

ANONYMOUS DYNAMIC SOURCE ROUTING (ANONDSR)

AnonDSR [6] routing consists of three protocols: security parameter establishment, anonymous route discovery, and anonymous data transfer. Christo Ananth et al. [10] discussed about a system, the effective incentive scheme is proposed to stimulate the forwarding cooperation of nodes in VANETs. In a coalitional game model, every relevant node cooperates in forwarding messages as required by the routing protocol. This scheme is extended with constrained storage space. A lightweight approach is also proposed to stimulate the cooperation.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

The protocol consists of two phases: RREQ phase and RREP phase. The anonymous data transfer protocol builds a cryptographic onion for anonymous communication data protection [13]. The protocol is only used when an anonymous route discovery protocol is completed. Each intermediate forwarding node checks whether the pseudonym of the data packet belongs to it and decrypts one layer of the data onion using its session key if it is on the anonymous route. It then changes the route pseudonym by its forwarding routing table, uses the decrypted onion instead of the received onion, and broadcasts the new packet locally. It discards the packet if it is not on the anonymous route. The procedure is repeated until the data packet arrives at the destination. A reverse anonymous communication data transfer from the destination to the source uses the reverse data is designed to meet the following objectives:

- Sender-, receiver-, and relationship anonymity.
- Untraceability and unlocatability.
- Anonymous yet secure neighbourhood authentication.
- Low cryptographic overhead and high routing efficiency.
- Resistance to a wide range of adversarial attacks. MASK [4] relies on a proactive neighbour detection protocol to constantly see the snapshot of its one-hop mobile neighbourhood. However, the MASK's neighbour detection protocol is identity-free. Each MASK node only knows the physical presence of neighbouring ad hoc nodes. This is achieved by a pairing-based anonymous handshake between any pair of neighbouring nodes. MASK uses a three-stage handshake for key exchanges among a node and its new neighbouring nodes. After the handshake, each pair of nodes shares a chain of secret key and locally unique LinkID pair which corresponds to the pseudonyms used during handshake. MASK does not use a global trapdoor. In the MASK's RREQ packet, source S explicitly puts in the destination node D's network ID. This saves the processing overhead to open the global trapdoor, thus sparing the need of end-to-end key agreement and results in a more efficient RREQ procedure. However, the security trade-off is that recipient anonymity is compromised by every RREQ receiver.

MASK

MASK [4] is designed to meet the following objectives:

1. Sender-, receiver-, and relationship anonymity.
2. Untraceability and unlocatability.
3. Anonymous yet secure neighbourhood authentication.
4. Low cryptographic overhead and high routing efficiency.
5. Resistance to a wide range of adversarial attacks.

MASK [4] relies on a proactive neighbour detection protocol to constantly see the snapshot of its one-hop mobile neighbourhood. However, the MASK's neighbour detection protocol is identity-free. Each MASK node only knows the physical presence of neighbouring ad hoc nodes. This is achieved by a pairing-based anonymous handshake between any pair of neighbouring nodes. MASK uses a three-stage handshake

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

for key exchanges among a node and its new neighbouring nodes. After the handshake, each pair of nodes shares a chain of secret key and locally unique LinkID pair which corresponds to the pseudonyms used during handshake. MASK does not use a global trapdoor. In the MASK's RREQ packet, source S explicitly puts in the destination node D's network ID. This saves the processing overhead to open the global trapdoor, thus sparing the need of end-to-end key agreement and results in a more efficient RREQ procedure. However, the security trade-off is that recipient anonymity is compromised by every RREQ receiver.

ASR (Anonymous Secure Routing)

The functionality of the ASR protocol proposed by Zhu et al is essentially the same as that of ANODR[3]. ASR makes no use of onion encryption as in ANODR that are built up as the Route request progresses through the network, but instead relies on state information that is kept at the forwarding nodes [5].

ALARM (Anonymous Location Aided Routing)

ALARM [8] uses nodes current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques (e.g., group signatures), ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and untraceability (tracking-resistance).Although it doesn't provide full security on the location anonymity of source and destination.

ALERT(Anonymous Location Based Efficient Routing)

Anonymous Location based efficient Routing Protocol in MANETs-ALERT proposed by Haiying Shen and Lianyu Zhao dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. ALERT offers anonymity protection to sources, destinations, and routes. 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[5]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. A notify and go mechanism is incorporated in order to have the source anonymity

AASR(Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments)

A new routing protocol, i.e., authenticated anonymous secure routing (AASR) [13], to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message, is

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

designed to prevent intermediate nodes from inferring a real destination. Simulation results have demonstrated the effectiveness of the proposed AASR protocol with improved performance as compared to the existing protocols.

Comparison of Anonymous Protocols

The first three aspects have significant performance impacts on mobile ad hoc routing:

1) Proactive neighbor detection effects periodic communication and computational overhead on every mobile node.

2) Because public key cryptography requires longer keys and more CPU cycles, using expensive public key cryptography (encryption/decryption) with expensive RREQ flood incurs severe communication and computational overheads per flood.

3)In MIX-net, a one-hop neighborhood is exposed to an internal (and possibly external) adversary. This is not a security problem in fixed networks, but in mobile networks, this reveals the changing local network topology to the mobile wireless adversary, which can quickly scan the entire network at once and obtain an estimation of the entire network topology.

5) Ensuring recipient anonymity (of the destination's network ID) is a critical security concern. Otherwise, every RREQ receiver can see how busy a destination node is. This traffic analysis can be used by the adversary to define the priority in node tracing attacks.

CONCLUSION:

ANODR which is compliant with its design principles- identity-free routing and on-demand routing is compared with the AnonDSR and MASK. But in these protocol also the requirement of network is not fully satisfied. The only protocol which satisfies the network requirement is Authenticated Anonymous Secure Routing Protocol (AASR).More specifically this protocol provides authenticate to route request packet by using group signature. Each of them has got its own merits and demerits due to the different techniques being used to achieve their goals. We give priority to AASR due to its inherent characteristics of providing anonymity to the network and improving and making it more efficient.Here we analyzed the other protocols that are related to these goals. We prefer to improve AASR by reducing the packet delay rather than creating a new protocol.

REFERENCES:

[1] C. Perkins, E. Belding-Royer, S. Das, et al., "RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing," Internet RFCs, 2003.

[2] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.

[3] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.

[4] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and on- demand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888–902, Aug. 2007.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

[5] Anupriya Augustine and Jubin Sebastian E,"A Study of Efficient Anonymous Routing Protocols in MANET," International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014 .

[6] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05), Nov. 2005.

[7] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951. [9] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

[8]K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," IEEE Trans. on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

[9] X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335–348, July/Aug. 2005.

[10] Christo Ananth, M.Muthamil Jothi, A.Nancy, V.Manjula, R.Muthu Veni, S.Kavya, "Efficient message forwarding in MANETs", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:6-9

[11] X. Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks," in Proc. IEEE MILCOM'06, Oct. 2006.

[12] Shino Sara Varghese, J. Immanuel John raja," A Survey on Anonymous Routing Protocols in MANET", Recent Advances In Networking, Vlsi And Signal Processing.

[13] Wei Liu and Ming Yu ," AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments",IEEE Transactions on Vehicular Technology, vol. x, no. y, March 2014 .