ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

# SURVEY ON FINDING END TO END COMMUNICATION FOR DISCOVERY SYSTEM IN MANET USING ANONYMOUS SUPERNODE

S.Mohideen Badhusha,
Assistant Professor/ CSE department,
K.S.Rangasamy College of Technology,
Tirunchengode, Tamilnadu, India.

J.Sobana, M.E(IInd Year)/CSE,
K.S.Rangasamy College of Technology,
Tirunchengode, Tamilnadu, India.

**Abstract**— Privacy and Security have emerged as an important research issue in Mobile Ad Hoc Networks (MANET) due to its unique nature such as scarce of resources and absence of centralized authority. There are number of protocols have been proposed to provide privacy and security for data communication in an adverse environment, but those protocols are compromised in many ways by the attackers. We identify a number of problems of previously proposed works and propose an efficient solution that provides anonymity in a stronger adversary model.

**Keywords:** Anonymous communication, mobile ad hoc networks.

## 1. INTRODUCTION

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. In ad hoc networks, the mobile nodes on the network dynamically establish the routing process by themselves. There is the possibility of more security threats in case of mobile and ad hoc networks (MANET) as compare to centralized wireless networks. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate [1], whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust. Basically there are two types of attacks.

Active attack: Active attack can be external or internal. They can disturb the network’s task by alarming the false message or modifying information [2]. Internal attacks are attacker within the network and external network are outside the network by carried out nodes that do not belongs to the network e.g. modification, jamming and message reply.

Passive attack: Passive attacks are difficult to detect and does not disturb the network’s performance or operation e.g. traffic analysis, traffic monitoring.

In order to achieve anonymous Communication in MANETs, many anonymous routing protocols such ANODR [3], MASK [4], and OLAR [5] have been proposed. Recently, statistical traffic

analysis Attacks have considerably been increasing due to their passive nature, i.e., attackers need only collect information and quietly perform analysis without changing the network behavior (injection or modifying packages). The predecessor attacks and disclosure attacks are two representatives. However, all of these previous approaches do not work well to analyze MANET traffic due to the following three natures MANETs: 1) The broadcasting nature: In wired networks [6], a point-to-point communication usually has only one possible recipient, In wireless networks, while a message is sent, multiple users can receive it simultaneously. 2) In MANETs which each mobile node can serve as a host and a router both. Thus, it is difficult to determine the role of a mobile node to be a source, a destination or a relay.
3) The mobile nature: Most of the existing traffic analysis models do not consider the mobility of the communication peers which makes the communication relationship between mobile nodes complex.

Generally, there are two types of MANETs exist: open and closed [12]. Closed MANETs don't have cooperation problems, since all nodes work towards a common goal and can easily be controlled. Open MANETs contain nodes that share their resources to ensure global connectivity but they many have different goals. The nodes in open MANETs are operated by multiple users, and they need not be forced to cooperate.

To protect user privacy and information security in MANETs, complete anonymity is the most requiring feature.Anonymity in terms of unlinkability, unobservability, and pseudonymity discussed in [13], are based on Item of Interest (IOI) including sender, receiver, content etc. These terms are discussed as follows:
(i) **Unlinkability:** Unlinkability of two or more IOI means that within the system from the attackers perspective, these IOI no more and no less related after his/her observation than they are related concerning his/her a priori-knowledge.
(ii) **Unobservability:** Unobservability is the state of IOI being indistinguishable from any IOI at all.
(iii) **Pseudonymity:** A pseudonym is an identifier of a subject other than one of the subject's real names.

## II. ROUTING PROTOCOLS OF MANETS

Many different routing protocols [20,21] have been developed for MANETs. They can be classified into two categories:

**Table-driven**: Table driven routing protocols essentially use proactive schemes. They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

**On-demand**: A different approach from tabledriven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Three main routing protocols for a MANET are destination-sequenced distance-vector routing protocol (DSDV), AODV, and Dynamic Source Routing protocol (DSR).

## III.LITERATURE REVIEW

**Reed et al** [7] proposed a timing attack focus on the delay on each communication path. If the attacker can monitor the latency of each path, he can correlate the messages coming in and out of the system by analyzing their transmission latencies.

**Song et al** [8] proposed a node flushing attacks (blending attacks, n-1 attacks), the attacker sends a large quantity of messages to the targeted anonymous system (which is called a mix-net). Since most of the messages modified and reordered by the system are generated by the attacker, the attacker can track the rest a few (normal) messages.

**W. Dai et al** [10] proposed a message tagging attacks; require attackers to occupy at least one node that works as a router in the communication path so that they can tag some of the forwarded messages for traffic analysis. By recognizing the tags in latter transmission hops, attackers can track the traffic flow. The watermarking attacks are actually variants of the message tagging attacks. They reveal the end-to-end communication relations by purposely introducing latency to selected packets.

**Kong and Hong et al** [11] proposed an Anonymous On-Demand Routing (ANODR) Protocol, is the first one to provide anonymity and unlinkability for routing in MANET. ANODR uses one-time public/private key pairs to achieve anonymity and unlinkability but fail to guarantee content unobservability.

**Raymond et al** [9] proposed a brute force attack tries to track a message by enumerating all possible links a message could traverse.

**Seys and Preneel et al** [14] proposed an Anonymous Routing Protocol (ARM) which uses one-time public/private key pairs and follows only anonymity in route discovery and data forwarding.

**Liu et al** [15] proposed a Hierarchical Anonymous Routing Scheme to provide Inter-group and Intra-group anonymity in Mobile Ad-Hoc Networks. This protocol controls the computational overhead using the hierarchical routing scheme and preserves routing anonymity.

**Zhang et al** [16] proposed Anonymous On-Demand Routing (MASK) which enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR, which is very sensitive to node mobility that may lower routing efficiency.

**Denh and Rex et al** [17] proposed On- Demand Anonymous Routing (ODAR) using public key cryptosystems for secure anonymous routing, but they assume that long-term public/private key pairs have been set up on each node for anonymous communication.

**Lin et al** [18] proposed An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks (ASRPAKE) to provide anonymity from all the intermediate nodes and also integrates the authenticated key exchange mechanisms into the routing algorithm design. The proposed protocol uses an efficient ring signature scheme based on ECC to achieve anonymous authenticated key agreement among mobile nodes in the network. This scheme suffers from route message flooding.

**Choi et al** [19] anonymous and secure reporting (ASR) of traffic forwarding activity in mobile ad hoc networks, make use of one-time public/private key pairs to achieve anonymity and unlinkability. ARMR uses one-time public-keys and bloom filter to establish multiple routes for mobile ad hoc networks and ASR is designed to achieve stronger location privacy, which ensures nodes on route have no information on their distance to the source/destination node.

**Gunasekaran and Premalatha et al** [13] proposed an Secure Onion Throat protocol provides privacy and security for data communication through complete anonymity in mobile ad hoc networks. To achieve complete anonymity, the SOT protocol implements the combination of group signature and onion routing with ID-based encryption for route discovery which prevents the different kinds of attacks which have been posed by adversaries.

**Pan and Li** [22] proposed an Efficient Strong Anonymous Routing (MASR) Protocol which uses onion routing scheme to achieve anonymity but suffers from routing overhead and computation cost.

**He et al** [23] proposed a timing-based Approach to trace down the potential destinations given a known source. In this approach, assuming the transmission delays are bounded at each relay node, they estimate the flow rates of communication paths using packet matching. Then based on the estimated flow rates, a set of nodes that partition the network into two parts, one part to which the source can communicate in sufficient rate and the other to which it cannot, are identified to estimate the potential destinations.

**Liu et al** [24] designed a traffic inference algorithm (TIA) for MANETs based on the assumption that the difference between data frames, routing frames, and MAC control frames is visible to the passive adversaries, so that they can recognize the point-to-point traffic using the MAC control frames, identify the end-to-end flows by tracing the routing frames, and then infer the actual traffic pattern using the data frames. The TIA achieves good accuracy in traffic inference, while the mechanism is tightly tied to particular anonymous routing protocols.

## IV. CONCLUSION

Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks. In this paper we first identified a number of problems and strengths in previously proposed solutions. We proposed a solution that provides stronger anonymity properties while also solving some of the efficiency problems. We also provide an analysis of how our protocol achieves its goals.

## REFERENCES

[1] Jaspinder Kaur, Birinder Singh "Detect and Isolate Black hole attack in MANET using AODV Protocol", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.

[2] Nirali Modi, Vinit Kumar Gupta "Prevention Of Black hole Attack using AODV Routing Protocol in MANET",International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.

[3] J. Kong, X. Hong, and M. Gerla "An Identity-Free and On- Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks", IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.

[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang "MASK: Anonymous On- Demand Routing in Mobile Ad Hoc Networks", IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.

[5] Y. Qin and D. Huang "OLAR: On-Demand Lightweight Anonymous Routing in MANETs", Proc. Fourth Int'l Conf. Mobile Computing and Ubiquitous Networking (ICMU '08), pp. 72-79, 2008.

[6] Yang Qin, Dijiang Huang "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions On Dependable And Secure Computing, Vol. 11, No. 2, March/April 2014.

[7] M. Reed, P. Syverson, and D. Goldschlag "Anonymous Connections and Onion Routing", IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 2002.

[8] R. Song, L. Korba, and G. Yee "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks", Proc. Third ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), pp. 33-42, 2005.

[9] 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, pp. 10-29, 2001.

[10] W. Dai "Two Attacks against a PipeNet-Like Protocol Once Used by the Freedom Service", http://weidai.com/freedomattacks. txt, 2013.

[11] J. Kong, and X. Hong "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks", in Proc. 4th International Symposium on Mobile Ad Hoc Networking & Computing, New York, 2003, pp. 291-302.

[12] H. Miranda, and L. Rodrigues "Preventing Selfishness in Open Mobile Ad Hoc Networks", in *Proc. 7th CaberNet Radicals Workshop*,Portugal, 2002, pp. 440-445.

[13] M. Gunasekaran, K. Premalatha "An Anonymity-Based Secure On-Demand Routing for Mobile Ad Hoc Networks", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:1, 2014.

[14] S. Seys, and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks," in Proc. of the International Conference on Advanced Information Networking and Applications, Vienna, 2006, pp. 133-137.

[15] L. Jun, H. Xiaoyan, K. Jiejun, Z. Qunwei, H. Ning, and G. B. Phillip "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks", in Proc. International Conference on Military Communication, Washington, 2006, pp. 1-7.

[16] Z. Yanchao, L. Wei, L. Wenjing, and F. Yuguang "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE Trans. On Wireless Communications, 5(9), pp. 2376 – 2385, Sep. 2006.

[17] S. Denh, C. Rex, and B. Lichun "ODAR: On-Demand Anonymous Routing in Ad Hoc Networks", in Proc. 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 2006, pp. 267-276.

[18] L. Xiaodong, L. Rongxing, Z. Haojin, H. Pin-Han, S. Xuemin, and C. Zhenful "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks", in Proc. IEEE International Conference on Communications, Glasgow, 2007, pp. 1247-1253.

[19] C. Heesook, E. William, S. Jaesheungn, D. M. Patrick, and F. L. P. Thomas "ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks", Wireless Networks, pp. 525-539, May- 2009.

[20] D. P. Agrawal and Q.-A. Zeng" Introduction to Wireless and Mobile Systems", Brooks/Cole Publishing, Aug. 2002.

[21] Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati "Routing Security in Wireless Ad Hoc Networks". IEEE Communications Magazine,October 2002.

[22] P. Jun, and L. Jianhua, "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Network," in Proc. International Conference on Management and Service

Science, Wuhan, 2009, pp. 1-6.

[23] T. He, H. Wong, and K. Lee, “Traffic Analysis in Anonymous MANETs,” Proc. Military Comm. Conf. (MILCOM ’08), pp. 1-7, 2008.

[24] Y. Liu, R. Zhang, J. Shi, and Y. Zhang “Traffic Inference in Anonymous MANETs”, Proc. IEEE Seventh Ann. Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON ’10), pp. 1-9, 2010.