Prabhu.K *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 11, November- 2014, pg. 125-130 **ISSN: 2321-8363**

A SURVEY ON VARIOUS METHODS IN MANET BASED ON ANALYSING VARIOUS TRAFFIC PATTERNS FOR ANONYMOUS COMMUNICATION

Prabhu.K[1], Gowtham.I[2], Dr. L.M.Nithya[3]

[1]PG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India, prabhuit.23@gmail.com

[2]PG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India, gowthaminbavanan@gmail.com

[3]Professor, Department of Information Technology, SNS College of Technology, Coimbatore, TamilNadu, India lmnithya@gmail.com

Abstract

Mobile Ad hoc Networks (MANETs) are a self configurable, Wireless and infrastructure independent network for mobile devices. MANETs have grown to be a challenging and attracting choice for disaster-response and military operations. Due to its ad hoc behaviour of networks, it permits fast operation and doesn't necessitate pre-defined network infrastructure. In such networks anonymous communications is a challenging topic which permits to exchange messages over communication parties on a network by without disclosing their identifiers of network to each other or to third parties. This type of Anonymous communications can be revealed by means of traffic analysis. Traffic analysis is an advanced approach which exposes relationships between users of anonymous communication systems. In this paper several anonymity enhancing techniques are surveyed for the protection of anonymity communication in mobile ad hoc networks (MANETs). The present survey includes various attacks and its corresponding protocols used for mitigating anonymous communication in MANETs. Finally comparative measures of each method are presented which provides the significance and limitations of each protocol on various attacks in mobile ad hoc networks (MANETs).

Keywords: Anonymous communication, Mobile ad hoc networks, Traffic analysis, ANODR.

1. Introduction

Mobile ad hoc networks (MANETs) have been developed into one of the fastest growing parts of research by means of its smaller, cheaper, and more powerful mobile devices. Due to the flexibility afforded by its dynamic infrastructure, MANETs are considered as attractive and advanced technology for various applications namely military, disaster-response, tactical and rescue operations. This new kind of infrastructure free network merges wireless communication along with high degree node mobility.

In contrast to conventional wired networks, MANETS holds no fixed infrastructure such as centralized management points, base stations etc. The combination of nodes in MANETs constructs an arbitrary topology. This form of flexibility formulates them to be more attractive for numerous applications such as military applications in which the network topology can vary rapidly to replicate a force's operational activities, and disaster recovery operations, whereas the conventional wired networks provides fixed infrastructure that might be non-operational in nature. The ad hoc nature of these networks makes the network as self-organisation and makes them appropriate for virtual conferences, whereas conventional network infrastructure is a time consuming and leads to high computational cost.

Traditional wired networks employ dedicated nodes to perform fundamental functions namely routing, packet forwarding and network management. Nodes on MANET's employ multi-hop communication that is nodes which are within other radio range may communicate via wireless links, whereas nodes that are at distant might rely on intermediate nodes which perform as routers to transmit messages. Due to the dynamic network topology, mobile nodes can migrate, disappear and links the network by frequently updating its routes.

In MANET, when any nodes exist within transmission range, point-to-point communication is used in which more than two mobile nodes can communicate with each other directly. Or else they will use intermediate nodes among the source and destination to bring the packets. At this point there is no centralized administrator is presented between the nodes. Consequently, a different node holds the routing and the management of resources in distributed mode. Thus MANETs is vulnerable under traffic analysis.

In MANET, statistical traffic analysis aims to determine sensitive information from the statistical characteristics of the network traffic namely traffic volume etc. Normally the adversaries do not alter the network performance by inserting or modifying packets. Those adversaries simply gather traffic information and execute statistical calculations. Traffic analysis is the procedure of interrupting and gathering messages by means to track significant information from communication patterns. That leaking of information is not altered by simply doing monitoring and analysis actions. It acquires information from the timing packets and monitor frequency. Particularly, this analysis is not only used for gathering information and but also employed to evade security systems in place. It is basically carried out in encryption and not only in decryption. Traffic analysis be capable of be explored in military and counter applications. In the earlier approaches, various traffic analysis attacks have been investigated for static wired networks. In this paper, recent methods of anonymous enhancing techniques are surveyed for traffic analysis in MANET.

The following literature describes each method precisely for mitigating various attacks in MANETS and in addition it describes pros and cons of each method are tabulated accordingly.

2. Analysing Various Traffic Pattern In Anonymous Communication Methods In Manet

2.1 Onion routing protocol

In [1] Michael.et.al presented onion routing prototype which can be employed to protect an Internet services against both traffic analysis attacks and eavesdropping from both the outside observers and network. They split the connection anonymity from the communication anonymity over that connection. For instance, when two parties operating onion routers which is able to recognize themselves to each other by without disclosing the existence of a connection between them. This work examines the adaptability of anonymous connections by extending their use in a various Internet applications. These applications comprise standard Internet services such as electronic mail, Web browsing and remote login. In addition Anonymous connections have also been used to hold virtual private networks (VPN) with connections that are opposing to traffic analysis which holds connectionless traffic. For supporting anonymous connections the configuration of onion routing network can be handled in different ways which includes customer-ISP configuration and firewall configuration, shifts privacy to the user's computer and may ease the carrier of responsibility for the user's connections.

2.2 Mask

In [2] Yanchao et.al presented framework of a new anonymous on-demand routing protocol, known as MASK, which can concurrently attain anonymous MAC-layer and network-layer communications. The originality of MASK relies in the exploitation of dynamic pseudonyms quite rather than network addresses and static MAC. MASK suggests anonymity of sender and receiver plus relationship anonymity of sender-receiver. Particularly, even if adversaries might examine a transmission of packets in which they neither establish real network IDs of its sender and receiver, nor they choose when some two nodes are communicating in the network. Additionally, MASK guarantees node as untrackability and unlocatability sense that, even though adversaries might identify some real network IDs or its group memberships, they are not capable to make a decision whom and where the related nodes are in the network. Furthermore, MASK warranties end-to-end flow untraceability, sense that forwarded packets are not traced by adversaries to its ending destination or backward to its new source, In addition they cannot identify packets corresponding to a original communication flow.

2.3 Anonymous on- Demand routing protocol

In [3] Jiejun et.al presented anonymous routing protocol known as Anonymous On-Demand Routing (ANODR) as the countermeasure. In real time, ANODR is a merely on-demand routing system that presently sets up desired anonymous routes. This restricts the possibility of traffic analyzing and eavesdropping to a critical time on-demand window. Generally in a mobile environment, few options are left for the adversary in whom they can instigate the attack in the critical time window or its corresponding information about the out-of-date of the

protected mobile nodes. An additional characteristic of ANODR is that it is the original identity-free ad hoc routing system, which is divergent to all earlier ad hoc routing system derived from node identities like MAC addresses and IP. In place of using node identities, one-time cryptographic trapdoors are relied on ANODR in routing. By without knowing node identities, the adversary cannot break a node's identity anonymity of mobile excluded by way of intrusion of node. This creates an immense physical dispute to the adversary.

2.4 MANET Anonymous Peer-to-peer Communication Protocol

In [4] Chao-Chin presented MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for peer to peer applications over mobile ad-hoc networks. This protocol is considered to be a flexible middleware connecting the MANET routing protocols and peer to peer applications. MAPCP utilizes a broadcast based method jointly with a probabilistic-based flooding control algorithm to launch anonymous paths among peers, which involves no hop-by-hop encryption or decryption, therefore entails lower power consumption and computational complexity. This protocol launches several anonymous paths among communication peers exist in a single phase of query, and is extremely resilient to node failure, mobility and malicious attacks. Moreover, MAPCP offers plans for communication peers to manage the trade off involving bandwidth efficiency and anonymity degree.

2.5 IEEE 802.11b-based manets

In [5] Dijiang et.al presented an approach of two-step unlink ability measurement for MANET. This approach provides a proof collection by means of statistical packet-counting traffic analysis and provides a confirmation of theory-based unlink ability measure. This work analyzed the wireless systems communication characteristics by employing IEEE 802.11b standards. Then proof collection and processing system is presented to obtain the traffic-communication relation matrix. With this matrix, an unlink ability of a given MANET is estimated by means of measuring a set of unlink ability. In contrast to Shannon information theory, this work is experientially observed that evidence theory highly relied on a well developed evidence collection method which accurately performs unlink ability evaluation. This constraint describes that the evaluator recognizes the infrastructure of the evaluating method and accurately defines the evidence and its accuracy which is being collected.

2.6 Traffic inference algorithm

In [6] Yunzhong et.al presented Traffic Inference Algorithm known as TIA, which permits a universal adversary to correctly infer the MANET traffic pattern regardless of the need of present anonymous on-demand routing protocols. TIA initially explores the frames of overheard routing for recognition of flow and then maps each flow in rounds according to the inter arrival times of data-frame. Given consecutive frames of a flow exceed, and then the consequent vectors of frame inter arrival times on some link is extremely correlated with that of the subsequent link by the side of the flow path. This makes the adversary to repeatedly obtain the unknown flows and therefore the traffic pattern from overheard frames of MAC includes no prior ideas of the inter arrival time distribution of each flow in a network. Even though traffic analysis based on inters arrival time has been generally carried out on low latency mix networks and its likelihood in anonymous MANETs still unaffected.

2.7 Energy efficient, secure and stable routing protocol

In [7] Sunil et.al presented Energy Efficient, Secure and Stable Routing Protocol, ad hoc network holds the hosts communicating between themselves with moveable radios. Due to the limited radio propagation range of this network which can be organized by without considering any infrastructure support or wired base station where routes are primarily considered as multi-hop. The ad hoc network nodes are limited by battery power for their function. A sufficient number of intermediate nodes are used to route a packet from a source to a destination. An efficient resource is said to be Battery power of a node which need to be employed proficiently so as to keep away from early termination of a network or a node. One unique characteristic of Energy Efficient ad hoc routing protocol is its exploitation of Power for each entry of route. For a certain option to reach a destination by means of two routes, a demanding node is essential to choose one with improved power status.

2.8 Anonymous Location-based Efficient Routing protocol

In [8] Haiying et.al presented Anonymous Location-based and Efficient Routing protocol (ALERT) for traffic analysis in MANET. ALERT forms a nontraceable anonymous route by dynamically splitting a network range

into zones and arbitrarily decides nodes in zones as intermediate relay nodes. Particularly, in each step of routing, a data sender divides the network environment so as to split themselves and the destination into two zones. After that it randomly picks a node in the rest zone as the subsequent relay node and employs the GPSR algorithm to forward the data to the relay node. Finally, the data is transmitted to k nodes in the zone of destination by offering k-anonymity to the destination node. Additionally, ALERT has a scheme to conceal the data originator between an amount of initiators to reinforce the anonymity defence of the source node. Furthermore ALERT is resilient to timing attacks and intersection attacks.

3. Comparative Table

The following comparative table shows the points of the merits and demerits of each surveyed method of various anonymity enhancing techniques used in MANETs for traffic pattern analysis.

Table 1: Comparison of various methods

S. No	Author and year	Attack	Technique/Protocol	Merits	De-Merits
1	Michael G. Reed, Paul F. Syverson, and David M. Goldschlag-2002	Eavesdropping and traffic analysis Attacks	Onion routing network prototypes	Efficiently analyses the traffic	Improved throughput is not obtained
2	Yanchao Zhang, Wei Liu, Wenjing Lou, and Yuguang Fang-2006	Message Coding, Flow Recognition, And Timing Analysis	MASK	Preserves the high routing efficiency, Highly effective and efficient	Routing information is not secured over internal adversaries, Results in Computational overhead
3	Jiejun Kong, Xiaoyan Hong, and Mario Gerla-2007	Node tracing attacks, packet flow tracing Attack	Anonymous on-Demand routing protocol.	Better trade-offs between routing performance and security protection is obtained	Performance of routing varies significantly when different cryptosystems are utilized
4	Chao-Chin Chou, David S. L. Wei, C.-C. Jay Kuo, and Kshirasagar Naik -2007	Passive attacks	MANET Anonymous Peer-to-peer Communication Protocol (MAPCP)	Results in lower computational complexity and power Consumption, Resilient to passive Attacks, Achieves a high anonymity degree	Increased overhead delay is resulted which arises due to increased number of route rediscover processes

5	Dijiang Huang-2008	Statistical packet-counting Traffic analysis (spta) attack	IEEE 802.11b-based MANETs	unlink ability evaluations of the 802.11b MANET is obtained efficiently, Prevents traffic analysis attacks	Scalability problem occurs
6	Yunzhong Liu, Rui Zhang, Jing Shi, and Yanchao Zhang-2010	Timing-analysis attacks	Traffic Inference Algorithm(TIA)	Resilience against traffic Analysis, Highlight the requirement for cross-layer designs	High cost of computational complexity is resulted
7	Sunil Taneja & Ashwani Kush-2012	Legitimate network users and malicious attackers	Energy Efficient, Secure and Stable Routing Protocol (EESRP)	Provides energy efficient, secure and stable routing strategy for MANETS, It is simple and flexible	QoS is not provided and it is supported in enhanced TCP connections
8	Haiying Shen, and Lianyu Zhao-2013	Intersection attacks and timing attacks	Anonymous Location-based Efficient Routing protocol (ALERT)	Offer high anonymity protection at a low cost,Achieve comparable routing efficiency	Not resilient to active attacks

4. Conclusion

The present survey presents various attacks and its corresponding protocols used for mitigating anonymous communication in MANETs. Each surveyed method is significantly efficient in terms of its corresponding performance metrics and resilient to various attacks. The presented literature shows the pros and cons of each method in various aspects. The efficiency of the surveyed method can be measured in terms of computational time, power consumption, computational complexity, overhead and throughput respectively. Thus the significance from each method is analysed properly and can be further exploited for analysing attacks of the Statistical Traffic Pattern Discovery System for MANETs.

References

[1]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.

[2]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.

[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]Chao-Chin Chou, David S. L. Wei, C.-C. Jay Kuo, and Kshirasagar Naik,"An efficient Anonymous communication protocol for peer to peer applications over Mobile Ad-hoc networks" IEEE Trans.Communication,vol 25, no, 1, 2007.

[5]D. Huang, "Unlinkability Measure for IEEE 802.11 Based MANETs," IEEE Trans. Wireless Comm., vol. 7, no. 3, pp. 1025-1034, Mar. 2008.

[6]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.
[7]Sunil Taneja & Ashwani Kush," Energy Efficient, Secure and Stable Routing Protocol for MANET", Global Journal of Computer Science and Technology, Volume 12 Issue 10 Version 1.0,2012
[8]Haiying Shen, and Lianyu Zhao," ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE TRANS. MOBILE COMPUTING, VOL. 12, NO. 6, 2013

