ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Review on Anonymous Routing Protocol for High Anonymity Protection in MANETs

Namrata R. Borkar, Prof. Avinash P. Wadhe

Student of M.E., Dept. of CSE., G.H.R.C.O.E, SGBA University, Amravati, Maharashtra, India

Assistant Professor, Dept. of CSE., G.H.R.C.O.E, SGBA University, Amravati, Maharashtra, India

ABSTRACT: Mobile Ad-Hoc Network (MANET) uses an anonymous routing protocol for security purpose. This protocol hides nodes original identity from outsider, so that observer cannot threaten the security of network. An anonymous communication method in MANETs is mostly classified into three type s reactive methods, proactive methods and anonymous routing technique. Other reactive routing techniques involves hop-by-hop encryption and redundant traffic routing .This routing methods either generate high cost or cannot provide full anonymity protection to sources, destinations, data and routes Mobile Ad Hoc Networks (MANETs) uses various anonymous routing protocols to support anonymity protection to sources and destination and data. Therefore to offer a high anonymity protection, Anonymous Location-based Efficient Routing protocol (ALERT) is proposed. Basic idea behind ALERT is to dynamically partition the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which creates a non-traceable anonymous route.

KEYWORDS: MANET, Anonymity Routing Protocols, Zone Partitions, ALERT.

I. INTRODUCTION

Fast development of Mobile Ad Hoc Networks (MANETs) excited numerous wireless applications that can be used in a wide number of areas. It has self organizing and independent infrastructures, uses such as communication and information sharing. MANETs feature self-organizing and independent infrastructures that makes them an ideal alternative for uses such as information sharing and communication. Because of the decentralization and openness features of MANETs, usually it is not desirable to constrain the membership of the nodes in the network. Nodes in the Mobile Ad-hoc Networks are vulnerable to malicious entities which tamper and analyse data as well as traffic analysis by communication eavesdropping or attacking routing protocols. In civil oriented applications, anonymity may not be a basic requirement. But in military applications, it becomes critical for example a soldier communication Consider a Mobile Ad hoc network environment deployed in a battlefield arena in Militaries. In which enemies may intercept transmitted packets, their nodes may attacks to commander nodes, and also they can be block the data transmission by comprising relay nodes through traffic analysis. So, to provide secure communication anonymous routing protocols plays vital role in MANETs which hides the node identities and also it by preventing traffic analysis attacks from outside observers.

MANETs includes Anonymity in terms of identity and location of data, source, destination and route. For source and destination it's very difficult to obtain the real identities and exact location of other nodes. Likewise, 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 has information about the real identities and locations of intermediate nodes en route. In order to dissociate the relationship between sender and recipient (i.e. relationship unobservability [1]), it is important to make an anonymous path between the two endpoints and make sure that nodes en route don't recognize where the endpoints are, particularly in MANETs where location devices might be equipped. In MANETs, existing anonymous routing protocols can be divided into two categories: redundant traffic [8] and hop by hop encryption. Public key based encryption and high traffic causes to generate significantly high cost, many of approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources. Additionally, many of the approaches in MANETs cannot provide all of the aforementioned anonymity protections. In existing protocol, ALARM cannot protect the location anonymity of source and destination [10], SDDR protects the location anonymity of source and destination but cannot provide route anonymity, and ZAP [11] only destination anonymity. Many anonymity routing algorithms [4] are based

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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 strict relay node selection of the protocol makes it easy to reveal the source and destination and to analyse traffic. MANETs' complex routing and stringent channel resource constraints impose strict limits on the system capacity. Also, the current increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency.

However, existing anonymous routing protocols produces a significantly high cost that exacerbates the problem of resource constraint in MANETs. A low quality of service in voice and video data transmission may lead to disastrous delay in military operations. Mobile Ad hoc Networks employing a high cost anonymous routing in a battlefield area, to provide high anonymity protection for source, destination, data and route with low cost, we propose a new protocol as an Anonymous Location based and Efficient Routing protocol (ALERT). The idea of ALERT is to dynamically partition a network field into groups. Here we call it as a "Zones" and then it randomly chooses nodes in Zones as intermediate relay nodes that create a non traceable anonymous route. Particularly, in every routing step, the sender or forwarder of data partitions the network field in order to separate itself and the destination into two different zones. It then arbitrarily selects a node in the other zone as the next relay node and uses the GPSR [4] to send the data to the relay node. The final step, the data is broadcasted to k -nodes that are present in the destination zone, which provides k anonymity to the destination. In addition, ALERT (Anonymous Location based and Efficient Routing protocol) hides the data initiator among a number of initiators to strengthen the anonymity protection of the source node. ALERT also provides protection against intersection attacks and timing attacks [13]. In summary, the contribution of this work includes:

1. Anonymous routing. ALERT provides identity, route anonymity, location anonymity of source and destination.
2. Low cost. Rather than relying on hop by-hop encryption and redundant traffic, ALERT makes use of randomized routing of one message copy to provide anonymity protection.
3. Resilience to timing attacks and intersection attacks. ALERT has a strategy to effectively prevent the intersection attacks.

II. LITERATURE SURVEY

i) L. Zhao and H. Shen, "ALERT: An Anonymous Location- Based Efficient Routing Protocol in MANETs" IEEE Transactions on Mobile computing Vol. 12 No. 6 June 2013[1]

Previous anonymous routing protocols, depending on either hop-by-hop encryption or redundant traffic which generates high cost. Also, some protocols are unable to provide complete anonymity protection to source, destination, and route. ALERT is differentiated by its anonymity protection for sources and low cost, routes and destinations. It makes use of dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the nodes en route and two endpoints. A packet in ALERT involves the source and destination zones rather than their positions to provide anonymity protection to the source as well as the destination. It 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. Also, it makes use of local broadcasting for destination anonymity. In addition to this, ALERT provides an efficient solution to counter intersection attacks.

ii) 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. [2]

In this paper, Zhi, Z. said "Due to the utilization of location information, geographic ad hoc routing presents superiority in scalability compared with traditional topology-based routing in mobile ad hoc networks". On the other hand, the consequent solicitation for location presence incurs severe concerns privacy of location, which has not properly studied. In this paper, we try to preserve privacy of location based on the idea of dissociating location information of the user 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.

iii) V. Pathak, D. Yao, & L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008[3]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

V. Pathak, D. Yao, and L. Iftode propose to secure location aware services over vehicular ad-hoc networks (VANET) with our geographical secure path routing protocol (GSPR). GSPR is an infrastructure free geographic routing protocol, which is resilient to disruptions caused by faulty or malicious nodes. Geographical locations of anonymous nodes are authenticated order to provide location authentication and location privacy simultaneously. This protocol also authenticates the routing paths taken by every individual message. This paper represents the structure of the GSPR secure geographic routing protocol.

iv) 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 said "Mobile Ad Hoc Networks (MANETs) are particularly useful and well-suitable for critical situations, such as law enforcement, military and emergency rescue and disaster recovery". Whenever operating in hostile or suspicious settings, MANETs needs communication security as well as privacy, specifically, in underlying routing protocols. This paper primarily emphasizes on privacy aspects of mobility. Unlike many other networks, where communication is based on long-term identities (addresses), we argue that the location centric communication paradigm is better-suited for privacy in suspicious MANETs. We construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries.

III. ROUTING PROTOCOLS IN MANETS

Several routing protocols have been suggested and used for MANET. Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable displacement of nodes. In General, current routing protocols for MANET can be categorized as:

A. *Proactive (Table-Driven):*

The pro active routing protocols are the same as current Internet routing protocols such as the RIP(Routing Information Protocol), DV(distance-vector),OSPF (Open Shortest Path First and link-state. They try to maintain consistent, latest routing information of the entire network. Each and every node has to maintain one or more tables to store its routing information, and must have to response to the changes in network topology by broadcasting this latest information. Several existing pro-active ad hoc routing protocols are: DSDV (Destination Sequenced Distance-Vector, WRP (Wireless Routing Protocol), CGSR (Cluster head Gateway Switch Routing), GSR (Global State Routing), FSR (Fisheye State Routing), HSR (Hierarchical State Routing), ZHLS (Zone based Hierarchical Link State), and STAR (Source Tree Adaptive Routing).

B. *Reactive (Source-Initiated On-Demand Driven):*

These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. Whenever a source needs to a destination, it has to perform a route by route discovery process, and also maintain it by some sort of route maintenance procedure until either the route is no longer desired or it becomes inaccessible. Finally, it is tearing down by route deletion procedure. Some existing active routing protocols are- [14].DSR (Dynamic Source Routing,), ABR (Associativity Based Routing), TORA (Temporally-Ordered Routing Algorithm), SSR Signal Stability Routing), PAR (Power-Aware Routing), LAR (Location Aided Routing), CBR (Cluster Based Routing), AODV (ad hoc On-Demand Distance Vector Routing,). In pro-active routing protocols, routes are always available with the consumption of signalling traffic and power. Whereas, re active protocols causes longer delay while route discovery process. Both types of routing protocols have been improving to be more secure, scalable and to support higher quality of service.

C. *Hybrid Protocols:*

Hybrid routing protocols [14, 15] aggregates a set of nodes into zones in the topology. After that, the network is divided into several no. of zones and proactive approach is used within each zone to maintain routing information. To transmit packets between different zones, the reactive routing approach is used. But, in hybrid approach, a route towards a destination that is in the same zone is established without any delay, while a route maintenance and a route discovery procedure is required for destinations that are in other zones. The zone routing protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue. Further, these types of routing protocols can provide a better trade-off between communication overhead and delay but this correlation is subjected to the dynamics of a zone and the size of a zone. Therefore, the hybrid routing protocol approach is a perfect

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

candidate for routing in a large network. At network layer, routing protocols are used to find route for packet transmission. The major advantage of a routing protocol can be studied through metrics-both qualitative and quantitative with which to measure its suitability and performance. There are number of Desirable qualitative properties of MANET. Some of this are- Loop-freedom, Distributed operation, Demand-based operation, Security, Sleep period operation Proactive operation, & unidirectional link support. Several quantitative metrics which can be help to assess the performance of routing protocol are- Percentage Out-of-Order Delivery, throughput, Route Acquisition Time, End-to-end delay and Efficiency. Important parameters that should be varied involves Network connectivity, Link capacity, Network size, Topological rate of change, Traffic patterns, Fraction unidirectional links, Fraction Mobility and frequency of sleeping nodes.

IV. ANONYMOUS ROUTING PROTOCOLS DESCRIPTION

Anonymous routing protocols are very crucial in MANETs to give secure communications by hiding node identities and preventing traffic analysis attacks from observers outside the network Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. `Location and identity anonymity of source nodes and destination nodes' means it is hard if possible for other nodes to obtain the real identities and exact locations of sources and destinations. For route anonymity, attackers, either en route or out of the route, cannot trace the flow of packet back to its source or to the destination, and none of the nodes have information about the true identities and locations of intermediary nodes en route. In order to dissociate the link between source and destination, it is important to form an anonymous path between the two end-points and make sure that nodes en route do not know about where the endpoints are, mainly in MANETs, where location devices can be equipped.

V. EXISTING ANONYMOUS ROUTING PROTOCOLS

A. *ALRAM*

The Anonymous Location Aided Routing in Suspicious MANETs is one of the anonymous routing protocols in MANET. ALARM find out problems in MANET. And also provide secure anonymous routing in network. For this it uses link state routing protocol. The LSR Takes nodes current position to broadcast and construct topology snapshots and forward data. For security issues, ALARM make use of advanced cryptographic techniques and it provides non-traceability, node authentication, data integrity privacy features. It also provides security against active and passive attacks. But problem with ALARM is it cannot protect location anonymity of source and destination node.

B. *ASR*

Another anonymous routing protocol is Anonymous Secure Routing (ASR) protocol. This protocol provides some additional properties of anonymity, such as Strong Location Privacy and Identity Anonymity. At the same time, it also ensures the security of discovered routes against various passive and active attacks. But ASR protocol having route anonymity problem.

C. *AO2P*

AO2P is one of the important anonymous routing protocols. It is an ad hoc on-demand position-based private routing algorithm. This protocol is mainly proposed for communicate on anonymity. In this instead of node identity, nodes position is used for route discovery.

VI. ALERT

The An Anonymous Location-based and Efficient Routing protocol (ALERT)[1] provides high anonymity protection for data, sources, destination, and route with low cost. It dynamically partitions a network field into zones and randomly chooses nodes in zones such as intermediate relay nodes that create a non-traceable anonymous route. Fig 1 shows different zone partitions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

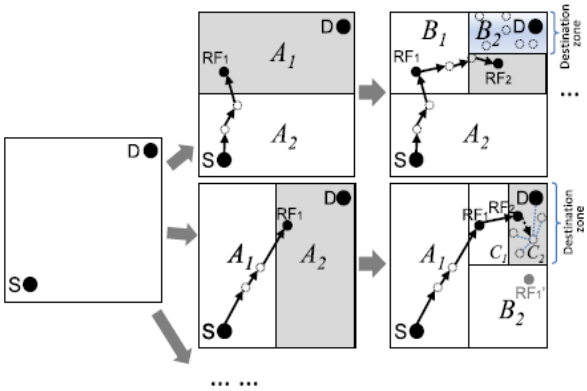

Fig. 1: Different Zone Partitions

Especially, in each & every routing step, a data forwarder or sender partitions the network field in order to separate itself and destination into two different zones. After that, it randomly selects a node in another zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the final stage, the data is broadcasted to k - nodes in the destination zone, which provides k- anonymity to the destination. In addition, ALERT [1] has a capability to hide the data initiator among a number of initiators to strengthen the anonymity of the source. Fig. 2 shows a routing among zones.

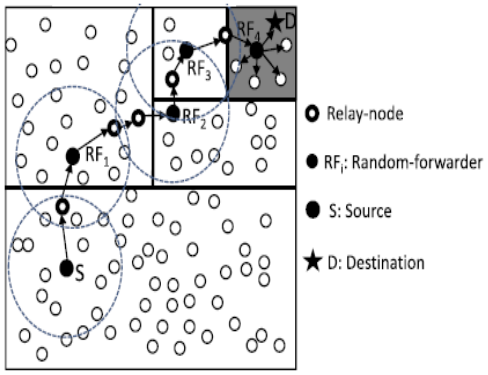

Fig. 2: Routing among zones

Also, ALERT is resilient to timing attacks Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The message's sender location may be revealed by merely exposing the transmission direction. Hence, anonymous communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Further, a malicious observer may attempt to block the data packets by compromising a no. of nodes, intercept the packets on a no. of nodes, or even trace back to the sender by detecting the data transmission direction. Thus, the route must be undetectable & untraceable. A malicious observer may attempts to detect destination nodes through traffic analysis by launching an intersection attack. Hence, the destination node also needs the anonymity protection.

1. Capabilities: by means of eavesdropping, the adversary nodes can analyze any routing protocol and can get information about the communication packets in their vicinity and positions of other nodes in the network. They can also trace data transmission on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can make attack on specific vulnerable nodes to control their behaviour, For example- with denial-of-service (DOS) attacks.

2. In capabilities: The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to all of the nodes. Their computing resources are limited. Thus, both symmetric as well as public/private key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

cannot be brutally decrypted within a reasonable time period. Thus, encrypted data are secure upto a certain degree when the key is not known to the attackers.

VII. CONCLUSION AND FUTURE WORK

Existing anonymous routing protocols depend on either hop-by-hop encryption or redundant traffic which generates high cost. And some protocols are not provides complete destination, source and route anonymity protection. ALERT is differentiated by its anonymity protection for sources and low cost, destinations, and routes. The ALERT makes use of 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. Every packet in ALERT involves 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 among a number of data initiators/ receivers.

REFERENCES

1. L. Zhao and H. Shen, 'ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs,' IEEE Transactions On Mobile Computing, June 2013.
2. Pfitzmann, M. Hansen, T. Dresden, and U.Kiel, 'Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.
3. Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, 'An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,' Proc. Int'l Symp. Applications on Internet (SAINT), 2006.
4. 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.
5. Y.-C. Hu, A. Perrig, and D.B. Johnson, 'Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,' Wireless Networks, vol. 11, pp. 21-38, 2005.
6. I Aad, C. Castelluccia, and J. Hubaux, 'Packet Coding for Strong Anonymity in Ad Hoc Networks,' Proc. Securecomm and Workshops, 2006.
7. K.E. Defrawy and G. Tsudik, 'ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,' Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.
8. 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.
9. T. Camp, J. Boleng, and V. Davies, 'A Survey of Mobility Models for Ad Hoc Network Research,' Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
10. 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.
11. S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, 'Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table,' Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.
12. X. Hong, M. Gerla, G. Pei, and C.C. Chiang, 'A Group Mobility Model for Ad Hoc Wireless Networks,' Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
13. 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 (WDIAU), pp. 10-29, 2001.
14. Priyanka Goyal, Vinti Parmar, Rahul Rishi, 'MANET: Vulnerabilities, Challenges, Attacks, Application', IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.
15. Belding-Royer, E.M. and C.K. Toh, 1999. 'A review of current routing protocols for ad-hoc mobile wireless networks', IEEE Personal Communication magazine pp: 46-55.

BIOGRAPHY

Ms. Namrata Ravindra Borkar is a Student of Master of Engineering in Computer Science & Engineering Department from G. H. Raisoni college of Engineering & Management, Amravati, Sant Gadge Baba Amravati University. I completed B.E. in Computer Science & Engineering from SGBAU, Amravati, MS, India. My research interests are Computer Networks and Network Security, etc.

Prof. Avinash P. Wadhe: Received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest includes Digital Forensics, Network Security, Data mining and Cloud Computing. He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.