ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 5|| May – 2016 ||
International Journal of Computational Engineering Research (IJCER)

A Study on Anonymous Routing Protocols in MANET

Akshayakumar satpathy[1],Geetidarshinipanigrahi[2] ,Manmathnath dash[3]
[1,3]*Associate Professor, Department of Computer Science Engineering, Gandhi Institute For Technology (GIFT), Bhubaneswar*
[2] *Assistant Professor, Department of Computer Science Engineering, Gandhi Engineering College, Bhubaneswar*

ABSTRACT
Mobile Ad hoc Networks (MANET) use anonymous routing protocols that hide node identities and routes from outside observers in order to provide anonymity protection. Existing anonymous routing protocols relay on hop by hop encryption or redundant traffic by generation high cost. The high cost exacerbates the inherent resource constraint problem in MANETs. Existing anonymous routing protocols provides full anonymity for the data sources, destinations, routing path with increased cost, delay. It consumes the bandwidth of the network. In proposed multicast routing scheme, the network field is partitioned into multicast zones and each zone has a zone head. The data packets will be transferred through the nodes which satisfies the position verification test and the zones through with the packet is transferred is dynamic. Routing misbehavior is mitigated using witness nodes. The proposed system is evaluated in terms of interruption, packet delivery ratio and energy consumption.
KEYWORDS- *MANET, Packet delivery ratio, interruption.*

I. INTRODUCTION

A mobile ad hoc network is a self-configuring infrastructure-less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". MANET is an autonomous collection of mobile users that communicate over relatively bandwidth-constrained wireless links. Network topology changes rapidly and unpredictably over time due to the mobility of the nodes. There arises the need of incorporating the routing functionality into nodes. MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. An ideal anonymous routing protocol for MANETs should have the followingproperties:

(1) We should not assume the knowledge of topological information about the network as accessing the topological information renders the system vulnerable toattacks.

(2) The identities and locations of the nodes in the route, and in particular, those of the source and the destination, should be hidden and protected.

(3) Multiple paths should be established to increase the difficulty of traffic analysis and avoid broken links due to nodemobility.

Anonymous protocols provide full anonymity for the data sources, destinations, and routes. An anonymous routing protocol does not consider the delay involved in the transfer of packets and bandwidth consumption. Limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. In order to reduce the delay in the transfer of packets, the routing path with the minimum number of hops must be selected. Verification tests are done to verify whether the selected hops are notmaliciousnodes. When the packet is transmitted through the shortest path, delay is reduced and the bandwidth of the other nodes will be saved.

II. LITERATUREREVIEW

A. Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-HocNetworks

Ranveer Chandra et.al (2001) proposed a method that improves the packet delivery ratio of the multicast routing protocol and decreases the variation in the number of packets received by different nodes. Gossip as a general technique has been used to solve several problems such as network news dissemination (NNTP), replicated data management, and failure detection. This method works in two phases, in the first phase, any suitable protocol is used to broadcast the message to the group of nodes. In the second concurrent phase, the gossip protocol tries to recover the lost messages. This gossip protocol is called Anonymous gossip. Anonymous

gossip does not require any member to know the other member of the multicast group. The node attempting to send the gossip message does not even know the identity of the node with which it will gossip until it sends the reply. Anonymous gossip is implemented over MAODV without much overhead. Buffer size is the limitation, when the old message gets stored in the buffer, there will be no place for the new messages, and the next limitation is the use of acknowledgment messages which is expensive in wireless networks.

B. Authenticated Routing For Ad HocNetworks

K. Sanzgiri et.al (2002) proposed the Authenticated Routing for Ad hoc Networks (ARAN) protocol that uses public-key cryptography instead of the shared security association. Each intermediate node running the protocol verifies the integrity of thereceived a message before forwarding it to its neighbor nodes. Source and destination nodes use certificates included in the route discovery and reply messages to authenticate each other. Alternatively, certificates can cost money, limiting the ability of the attackers to request them limitlessly. A short lifetime on certificates can also help manage the network. The protocol has an optional second discovery stage that provides non-repudiating route discovery.

C. Anonymous on Demand Routing with Untraceable Routes for Mobile Ad hocNetworks

J. Kong et.al (2003) proposed an approach that consists of three phases. Anonymous route discovery, Anonymous route maintenance, and Anonymous route forwarding. The route discovery phase includes a route request and route reply message. It implements

1) symmetric key agreement between two consecutive RREP forwarders and 2) enforces destination-initiated RREP procedure. The global trapdoor holds secret information for the intended destination and a public commitment for the same destination. RREP proof (or receipt) from the destination is obtained to prevent an adversarial network node to send back fake RREPs to disrupt ANODR. For the maintenance of the anonymous route, the routing table entries are recycled upon timeout T. The performance of ANODR decreases when the mobility of the nodes increases. Trapdoor information is used in this but it is not practical since the destination node does not know which shared session key should be used for the trapdoor if the destination node has many shared session keys.

D. Secure Efficient Distance Vector Routing For Mobile Wireless Ad HocNetworks

Yih-Chun Hu et.al (2003) proposes a scheme based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denial of- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, an efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios tested and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even despite any active attackers or compromised nodes in thenetwork.

E. An Efficient Secure Distributed AnonymousRouting Protocol for Mobile and Wireless Ad HocNetworks

A. Boukerche et.al (2004) proposed a protocol that allows only the trustworthy nodes to participate in transmission. It does not require the source node to gather information about the topology of the network. The source node broadcast the path discovery message with some trust requirement, the intermediate nodes satisfying the trust, inserts its ID and session key into the message, and encrypts the message. This message reaches the destination and the message gets decrypted in each intermediate node and reaches the source. The source node obtains complete information about the intermediate nodes. This protocol uses a multi cast mechanism and layered encryption. SDAR is not secured against Denial of Service attack. Messages are large and depend upon the number of hops. This protocol also limits theefficiency.

F. Mask

Y. Zhang et.al (2005) say that anonymous authentication with low cryptographic overhead and high routing efficiency can be obtained by using proactive neighbor detection. It is resistant to a wide range of adversarial attacks. MASK relies on a proactive neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. MASK's neighbor detection protocol is identity-free. Each MASK node only knows the physical presence of neighboring ad hoc nodes. This is achieved by a pairing-based anonymous handshake between any pair of neighboring nodes. MASK uses a three-stage handshake for key exchanges among a node and its new neighboring 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 for 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. The routing information is not authenticated. An already established path may consist of several multipath channels however the source and the destination nodes becomeunauthenticated.

G. Discount Anonymous on Demand Routing For Mobile Ad Hoc Networks

Liu Yang et.al (2006) provides the same mechanism of ANODR, but at a lower cost. It uses the same techniques used in ANODR. It has the benefit of achieving substantially lower computation and communication complexities at the cost of a slight reduction of privacy guarantees. Route requests in Discount- ANODR bear strong similarities to the Route request in ANODR with the limitation that intermediaries only know the destination of the request and the identity of the previous intermediary but not the originator of the request.

H. On Delivery Guarantees of Face and Combined Greedy- Face Routing In Ad Hoc and SensorNetworks

Hannes Frey et.al (2006) say specifically in relative neighborhood and Gabriel graphs recovery from a greedy routing failure is always possible without changing between any adjacent faces. This approach discusses face routing variants which simply restart face routing whenever the next face has to be explored. It is the first complete and formal proof that several proposed face routing and combined greedy face routing schemes do guarantee delivery in specific graph classes or even any arbitrary planar graphs. This method also discusses the reasons why other methods may fail to deliver a message or even end up in a loop. Traversing that face can be done by left hand, right hand, or alternating left/right-hand rule as it isfollowed.

I. Anonymous Authentication Protocol in Mobile Ad Hoc Networks

Tomasz Ciszkowski et.al (2006) proposed an Anonymous Authentication protocol which is enhanced with a distributed reputation system. The reputed distributed system is incorporatedwith trust management. Reputation depends on the time, own past experience, second-hand information and it is expressed by the level of trust. The end to end anonymous authentication is conducted in a three-phase handshake. The three phases are Anonymous authentication initialization, Anonymous reply, and Anonymous authentication. After the successful authentication, multiple anonymous data channels are established. The computational impact on the nodes is high.

J. A Group Mobility Model for Ad Hoc WirelessNetworks

Xiaoyan Hong et al. (2006) present a survey of various mobility models in both cellular networks and multi-hop networks. The group motion occurs frequently in ad hoc networks and introduces a novel group mobility model – Reference Point Group Mobility (RPGM) - to represent the relationship among mobile hosts. RPGM can be readily applied to many existing applications. Moreover, by proper choice of parameters, RPGM can be used to model several mobility models that were previously proposed. One of the main themes of this paper is to investigate the impact of the mobility model on the performance of a specific network protocol or application. To this end, the RPGM model to two different network protocol scenarios, clustering and routing, and have evaluated network performance under different mobility patterns and for different protocol implementations. When the mobility of the node increases, the overhead also increases. This shows how the mobility affects theperformance.

K. Efficient Anonymous Dynamic Source Routing For Mobile Ad-HocNetworks

Ronggong Song et.al (2007) provides three levels of security protection. This routing consists of three protocols. The first protocol is used to create a shared key and a nonce between the source and the destination for the secure communication. The second protocol uses the shared key and the nonce to create a trapdoor and employ anonymous onion routing between the source and the destination. In the last protocol, the source and the destination use their session key shared with the intermediate nodes to encrypt all communications with the cryptographic onion method. It offers good scalability. The anonymous route establishment depends on the number of hops between the source and the destination if the number of hops increases time will be alsoincreased.

L. Anonymous Location-Aided Routing In Suspicious Manets

K.E. Defrawy et.al (2007) uses the current location of the nodes for communication rather than their IDS. With the current location of the nodes, a secure MANET map is constructed, based on the current map, each node can decide which other nodes it wants to communicate with. It satisfies strong security policies and strong privacy policies. This approach uses group signatures which can be viewed as traditional public-key signatures. Any member of a large and dynamic group can sign a message and thereby producing a Group

signature. The group manager can open the group signature and find the actual signer. This feature is called as Escrowed Anonymity. This approach works only if the speed of the movement of nodes is nothigh.

M. Secure Location Verification for Vehicular Ad-Hoc Networks

Joo-Han Song et.al (2008) discuss the position spoofing attack. A novel Secure Location Verification (SLV) scheme is proposed to detect and prevent position-spoofing attack. SLV uses distance bounding, plausibility checks, and ellipse-based location estimation to verify the claimed location of a vehicle. Simulation results show that the proposed SLV scheme has a better performance than both autonomous position verification (APV) and greedy forwarding algorithms. It has three steps. RF-based distance bounding technique is used to bound the minimum distance between verifier V and proves P. Since RF signals travel at the speed-of-light c, V can prevent an attacker from reducing the measured distance by measuring the time of flight (ToF) of challenge-response messages between V and P. Since P can only cheat on its response message by appearing further from V than its actual location, any attempt to reduce the distance will be detected by V. When V estimates the distance to P, V also considers the non-zero processing delay _ of V
.The second step has three stages Acceptable transmission range, Acceptable speed limit, Roadway map. SLV can guarantee the minimum distance between fake and estimated location of proves by a certain value.

N. Packet Coding For Strong Anonymity in Ad Hoc Networks

ImadAad et.al (2008) provides a combined approach of multicasting and onion routing. By combining these two techniques the anonymity protection becomes more robust and complete. Each node has a publicly known identifier (ID), which is not necessarily an IP address. Nodes have limited battery and processing power. Initially assumption is that nodes are fixed. Two types of network devices: Tamper-resistant and non-tamper-resistant. In the first the assumption is that attackers can eavesdrop communications; analyze the traffic etc., while not being able to compromise secret keys in the network devices. In the second case, the assumption is that attackers can compromise any number of nodes along with the keys stored within. Nodes collaborate to forward packets even when ignoring the source and destination IDs. Checking the authenticity of a packet is possible (while still ignoring the source and destination IDs) when using tamper-resistantdevices.

O. Privacy Friendly Routing In Suspicious Manets

El Defrawy et.al (2008) focused on the privacy aspect of mobility and proposed a routing protocol, PRISM, which achieves privacy and security against both outsider and insider adversaries. Unlike most networks, where communication is based on long-term identities, the location-centric communication paradigm is better- suited for privacy in suspicious MANETs. Simulation results compare PRISM with an alternative location-centric link-state approach and show that PRISM generally achieves better performance under reasonable communication assumptions. The results reveal that PRISM is more computationally efficient and offers better privacy. PRISM'S route discovery takes a long time and requires more messages.

P. Secure Probabilistic Location Verification in Randomly Deployed Wireless SensorNetworks

E. Ekici et.al (2008) proposed Probabilistic Location Verification (PLV) algorithm leverages the probabilistic dependence of the number of hops a broadcast packet traverses to reach a destination and the Euclidean distance between the source and the destination. A small number of verifier nodes are used to determine the plausibility of the claimed location, which is represented by a
real number between zero and one. Using the calculated plausibility metric, it is possible to create an arbitrary number of trust levels in the location claimed. Simulation studies verify that the proposed solution provides high performance in the face of various types of attacks. The salient properties of the PLV algorithm can be summarized as follows: Sensor nodes do not need to be equipped with specialized hardware, Only a small number of specialized verifiers are needed, The plausibility of a location claim is expressed as a real number, not a hard binary decision, The PLV algorithm is resilient against some attacks and provides graceful degradation in performance. The main idea behind the proposed mechanism is to leverage the statistical relationships between the number of hops in a sensor network and the Euclidean distance that is covered. The so-called hop-distance relationship for linear sensor networks and possible extensions to two-dimensional networks has been proposed. This method is applicable for dense sensor networks.

Q. Anonymous Routing Protocol for Mobile Ad Hoc Networks

StefaanSeys et.al (2009) present an anonymous on-demand routing scheme for MANETs. The source and the destination share a secret key KSD and a secret pseudonym. The source will include this pseudonym in the route request message. The destination will have a list of pseudonyms used by different sources in its memory and it verifies whether the message is targeted at it or not. This pseudonym can be used only once (for a single route request message). The destination sends the reply with the same pseudonym. On the receipt of the

reply message source starts to send the data along with the onetime identifier attached with them. One time identifier protects the data from the attacker. Delay increases when the network size islarge.

R. Achieving Efficient Anonymity in Manets by Combining HIP, OLSR, andPseudonyms

Javier Campos's et.al (2010) proposed a protocol HOP and implemented it and it is based on cryptographic Host Identity Protocol (HIP) which offers security and user-level anonymity. Some enhancement is done to the authentication process to achieve Host Identity Tag (HIT). HIP protocol is combined with the OLSR routing protocol to achieve the support for a pseudonym. It uses multiple IP addresses per station (one per destination) to achieve a higher degree of anonymity when communicating. When two nodes wish to establish a secure connection, each will select a free IP address from its IP address pool that is used as a pseudonym for that connection. This approach is lightweight and it is easy to implement. It maximizes the performance. The maximum data encryption rate was limited to 12 Mbit/s.

S. Position-Based Routing In Mobile Ad-HocNetworks

SimardeepKaur et.al (2012) proposed a method of routing protocol using GPS**.** Hybrid protocols are used which combines the advantages of both reactive and proactive protocols. Position-based routing thus does not require the establishment or maintenance of routes. Location services can be classified according to how many nodes host the service. The position information can be collected in different ways. It can be collected from the direction and strength of the received wireless signals and through interfacing with a low- power Global Positioning System (GPS) and a satellite updating the positions of the nodes by sending signals to this GPS device. It hasdisadvantages like the problem of designing location update schemes to provide accurate destinationinformation.

T. Hybrid Anonymous Location-Aided Routing Protocol for Privacy-Preserving and Authentication inManet

Y.V.S.Saipragathi et.al (2013) uses both proactive and reactive mode of anonymous location-based routing. Proactive mode applies to the nodes within the predefined radius and this involves the construction of topology tables of the nodes. Reactive mode is applicable for the nodes outside the predefined radius and this involves route discovery process by broadcasting route request message and getting a route reply from the intermediate nodes. Group head node is selected in the network based on maximum connectivity. Building a topology table is difficult in mobile networks. This technique reduces the delay when compared to other anonymousprotocols.

III. PROPOSEDSYSTEM

In the proposed system once, a node receives a multicast packet, it divides the network into multicast regions. Some nodes manage the multicast zones and act as the zone heads. Nodes join and leave a zone by sending "join" and "leave" packets to the zone head. Join and leave packets are multicast packets with destination lists that contain only the zone head address. Zone Management supports Many-to-Many multicast mode, and thus every node in a multicast zone can multicast packets to all other nodes in the same zone. In the case of nodes joining or leaving, the zone head must send "update" packets including a list of its updated multicast zone members to all zone nodes. Nodes send "join" packets periodically to the zone head, and nodes that die without sending "leave" packets are removed from the list after a time-out period.

In order to detect the packet dropping by the misbehavior node, the nodes that are in contact maintains a contact record which includes which packets are in their buffers before data exchange, and what packets they send or receive during the data exchange. The record also includes the unique sequence number that each of them assigns for this contact. The record is signed by both nodes for integrity protection. They select witness nodes and send their records to the witness nodes; the witness node detects if there is any inconsistency.

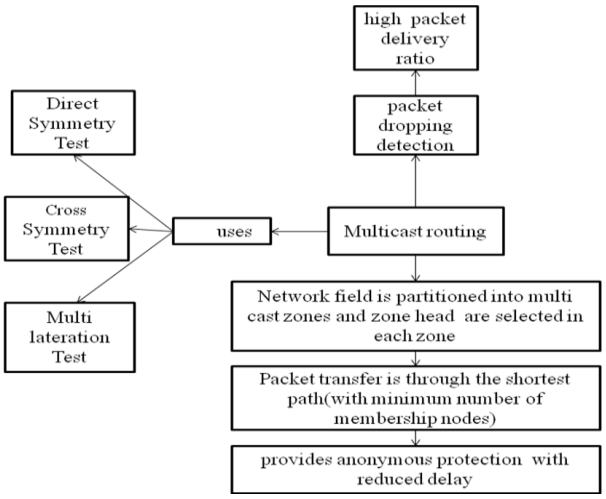

Fig.1 System architecture

IV. CONCLUSION

All the anonymous routing protocols discussed in the literature survey focus only on providing anonymous protection to the data sources, destination, routes. Most of the anonymous routing protocols provide anonymous protection with an increase in delay and consume the bandwidth of the mobile nodes. The proposed system aims to reduce the delay and saves the bandwidth of the mobile nodes.

REFERENCES

[1]. HaiyingShen, LianyuZhao,"ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs" IEEE Transactions On Mobile Computing, Vol.12, No. 6, JUNE2013.

[2]. AzzedineBoukerche, Khalil El-Khatib, Li Xu, Larry Korba," An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks" Computer Communications 28 (2005) 1193– 1203, September2004.

[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, K. and G. Tsudik, "PRISM: Privacy friendly Routing in Suspicious Mantes". Proceedings of the IEEE International Conference on Network Protocols, Oct. 19-22, IEEE Xplore Press, Orlando, FL., pp: 258-267. DOI:10.1109/ICNP.2008.4697044,2008.

[5]. Ekici, S. Vural, J. McNair, and D. Al-Abri," Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks,"ElsevierAdHocNetworks,vol.6,no.2,pp.195-209,2008.

[6]. Z. 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),2006.

[7]. Hannes Frey and Ivan Stojmenovic," On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor Networks" IMADA, University of Southern Denmark, SITE, University of Ottawa, 2006.

[8]. ImadAad, Claude Castelluccia, Jean-Pierre Hubaux," Packet Coding for Strong Anonymity in Ad Hoc Networks", I. Aad, C. Castelluccia, and J. Hubaux, "Proc. Securecomm and Workshops,2006.

[9]. Javier Campos, Carlos T. Calafate,MargaN´acher, PietroManzoni, and Juan Carlos Cano," HOP: Achieving Efficient Anonymity in MANETs by Combining HIP, OLSR, and Pseudonyms", Hindawi Publishing Corporation EURASIP Jour on Wireless Communications and Networking Volume 2011, Article ID 437868, 14 pages, 1 September 2010.

[10]. J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302,2003.

[11]. Ranveer Chandra, VenugopalanRamasubramanian Kenneth P. Birman," Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks", Proc. Securecomm and Workshops2001.

[12]. Ronggong Song, Larry Korba, George Yee" AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks", Proceedings of the 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks,2007.

[13]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M.A Belding- Royer," A Secure Routing Protocol For Ad Hoc Networks", in: Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November,2002.

[14]. J.-H. Song, V. Wong, and V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," Proc. IEEE Globecom, Dec.2008.

[15]. StefaanSeys and Bart Preneel."ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks", Computer Communications 28 (2005) 1193– 1203,2009.

[16]. SimardeepKaur, Anuj K. Gupta," Position Based Routing in Mobile Ad- Hoc Networks", IJCST Vol. 3, Issue 4, Oct - Dec 2012.

[17]. Y.V.S.Saipragathi, S.P. Setty," Hybrid Anonymous Location-Aided Routing Protocol For Privacy Preserving And AuthenticationIn

[18]. Manet", Journal of Theoretical and Applied Information Technology, Vol.55No.2,20thSeptember2013 .

[19]. Tomasz Ciszkowski and ZbigniewKotulski," ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Networks" Warsaw University of Technology,2006.

[20]. Yih-Chun Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[21]. L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops,2006.

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