Secured On-Demand Position Based Private Routing Protocol for Ad-Hoc Networks

Ramya.R , Shobana.K, Thangam.V.S

ramya_88@yahoo.com, kshobsi@yahoo.co.in ,thangam_85@yahoo.com

Department of Computer Science,
College of Engineering, Guindy, Anna University,
Chennai ,India

Abstract - Protecting personal privacy is important in Ad Hoc networks for improved security. This can be done by maintaining node anonymity so that it becomes difficult for adversaries to trace their potential victims. In this paper,an ad hoc, secured, on-demand, position-based, private routing protocol namely ASOP is proposed. Here, the positons of the destinations are the only position information disclosed in the network for routing discovery. A route is discovered by delivering a routing request message from the source towards the position of the destination. To determine the next hop with limited position information, the "Receiver Contention Channel Access Mechanism" is used. Pseudo IDs are used for data packet delivery after the route is set up. Real node IDs for destination, source and intermediate nodes are kept private in this protocol. A node's Pseudo ID is the result of the hash function of its position and time. The possibility that two nodes have the same pseudo Id is negligible since it is unlikely that two ad hoc nodes are at exactly the same position. Destination mobility is handled by Alert-Messaging system. Also,malicious nodes are identified by installing WatchDog and PathSelector on every server. Malicious nodes are those that become part of the route, deviate from expected behaviour and drop data packets. The contention scheme proposed in ASOP Protocol is vulnerable to malicious nodes that try to become part of the route by claiming False Identities for themselves. Such nodes are called as SYBIL NODES. These Sybil nodes are handled in this paper.

Index Terms - Anonymity, Privacy, Contention , Malicious nodes , Destination mobility

I. Introduction

While in wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not the case in an ad hoc network. Thus, routing is needed to find a path between source and destination and to forward packets appropriately. In Traditional Routing Algorithms like AODV[1], DSR[2], DSDV[3],a node has to disclose its ID in the network for building a router.Node activities such as sending or receiving data is highly traceable. Nodes are vulnerable to attacks and disruptions. Routing schemes rely on the cooperation and information exchanged among the nodes

More recently, there has been a growing focus on a class of routing algorithms that rely largely or completely on location information(based on position). These algorithms are commonly referred to as "POSITION-BASED ROUTING ALGORITHMS"[4]. Here in addition to node ID,extra information such as positions of the nodes is used for making routing decisions. Since it is unlikely for 2 ad hoc nodes to stay at the same position concurrently, the match between a position and ID is definitely unique.Hence, in these algorithms , when positions are revealed for routing , there is no need of node IDs. Hence node anonymity can be maintained.However such algorithms rely on

position exchange among the neighbouring nodes. Such time based position exchange messages make a node highly traceable. The trajectory of a node movement can be well known to other nodes even when its node ID is intentionally hidden. Hence there is lack of privacy in traditional position based ad hoc routing algorithms.

To achieve communication anonymity in position based routing schemes, ASOP is proposed. Here , the destination's position alone is revealed for routing purposes thereby maintaining the privacy of other nodes IDs. For routing discovery, a node sends out a routing request. Its neighbouring nodes receive the request and contend to access the channel for becoming the next hop using Receiever Contention Channel Access Mechanism. A receiver that is geographically closer to the destination is assigned a higher priority and can win the contention. Once the route is built, only Pseudo IDs are generated and are used by the nodes participating in the route. Nodes that get the access to the channel by winning the contention may maliciously drop packets. To avoid such nodes from becoming part of the route, WatchDog and PathSelector are used. Certain nodes may try to win the contention by reporting false Pseudo IDs as their own ID. To identify such nodes, a method of direct validation is proposed.

II. Related Works

Traditional Ad hoc Routing algorithms have been studied.. The major differences between these algorithms and traditional routing algorithms for wired networks are discussed.

Anonymous communication in ad hoc network has been studied in [4]. Here, once a route is found, pseudo-random numbers are used as temporary ID for the nodes along the route. Each node only knows the pseudo numbers from its previous hop and next hop. The communication privacy is achieved because real IDs are not revealed.

Position based routing in Ad hoc networks has been studied[5]. The position-based routing algorithms depend on the position availability. Especially, it is assumed that a source is able to get the position of its destination.

An on-demand position-based protocol namely AO2P is presented in [6]. This protocol maintains user anonymity by revealing only the destination's position information. A route is set up only when a source has data to send to a destination. system. Node mobility enhances destination anonymity by making the match between a node ID and a position temporary. To further improve destination privacy, R-AO2P is proposed, in which the position of a reference point, instead of the position of the destination, is used.

Malicious nodes are described in [7]. This paper deals with Misbehaving nodes and solutions to avoid such misbehaving nodes from becoming a part of the route. Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes.

In order to identify Sybil nodes , various methods have been discussed in [8].

In [9], each node has a geographical region around a fixed center. The region is called a virtual home region (VHR), and the ad hoc node updates its position information to all the nodes residing in its VHR. The relationship between a node ID and the fixed center of its VHR follows a Hash function, so that other nodes can acquire a node's position by sending request to the right VHR.

III. Our Proposal

ASOP ROUTING ALGORITHM

A.Position Management

We use a Virtual Home Region(VHR) based distributed secure position service system. An Ad Hoc node is assumed to be able to obtain its own geographic position. It is assumed that a source is able to get the position of its destination. Each node has a geographical region around a fixed center called the Virtual Home Region(VHR)[9]. The relationship between a node ID and the VHR follows a hash function that is predefined and known to all the nodes who join the network.

A number of servers which are also ad hoc nodes are distributed in the network. A node updates its position to the servers located in its VHR to which other nodes send position requests acquiring this node's position. Only a small

number of trusted nodes can act as position servers. A node updates its position to its VHR when the distance between its current position and the last reported position exceed a threshold value. When the source gets the position of its destination, it also gets the time when the position is updated and an authentication code. The time is needed for accuracy and the code can be any random number generated and sent to the position server by the destination.

B. ASOP Routing Discovery

Here, a source discovers its route through the delivery of a routing request to its destination. To find the route to its destination, the source first generates a Pseudo ID for itself through a globally defined Hash Function using its position and current time as its inputs. This procedure makes the probability of 2 active nodes having the same pseudo ID negligible. The source then sends out a Routing Request(rreq) message that carries Position of the destination , distance from this source to the destination and the source Pseudo ID.

The neighbouring nodes around the source called receivers will receive rreq. A receiver checks to find out whether it is the intended destination. If not, it uses the hash function to generate its own Pseudo ID. The receivers then contend for the wireless channel to send out the hop reply- hrep message.This contention mechanism called the hrep Contention Mechanism is discussed very soon. The receiver who has successfully sent out the hrep will be the next hop. Its pseudo ID is carried in the hrep. On receiving the hrep, the source replies with a confirm message(cnfm). Its next hop replies to this message with an ack. On receiving this ack, the source saves the pseudo ID in its routing table.

On receiving the cnfm message, the next hop receiver becomes a sender. The searching for the next hop is continued until the destination receives the rreq message. Finally, the destination sends out a Routing reply(rrep) message through the reverse path to the source. The destination also finds the corresponding authentication code according to the position carried in the rreq and encrypts the code with the secret key of its secret key pair.The encrypted result is included in the rrep and sent to the source.The source finds out whether it reaches the right destination by decrypting the information with the destination's key and comparing the authentication code with the one it obtained through the position request.

C.Receiver Contention Channel Access Mechanism

The receiver contention mechanism used in hrep contention phase is EY-NPMA (Elimination Yield Non Preemptive Priority Multiple Access). Here, the receivers are classified based on how much closer(geographical distance) they can move the rreq from the sender toward the destination. Based on this distance, priorities are assigned to the different nodes.

The hrep contention phase is divided into 3 phases:

Prioritization Phase :

This phase allows only the receivers with highest channel access priority among the contending nodes to participate in the next phase. A number of slots ,the same as the number of different priority classes are available in this phase. A receiver of priority 3 can send a burst slot 3 only if no burst is sent in the previous 2 slots. This means it has the highest priority. It therefore enters the next phase. If a receiver senses a burst in one of the previous slots, it will quit from hrep contention, cannot enter the next phase and therefore drop rreq.

Elimination Phase:

This phase starts immediately after the transmission of the prioritization bursts and consists of a number of slots.A receiver in this phase will transmit burst in a randomly selected slot. The receiver transmitting the longest series of bursts will survive. After the end of burst transmission, each receiver senses the channel for the duration of the elimination survival verification slot. If the channel is sensed to be idle, the receiver is admitted to the next phase. Otherwise, it drops itself from contention.

Yield Phase :

In this phase, a receiver will yield for a number of slots and listens to the channel and if the channel is sensed idle, it sends out a hrep. Otherwise ,the receiver loses contention and drops the rreq. |When more than one receiver sends out an hrep at the same time, a hrep collision occurs. The sender will have to resend the rreq in such cases.

In ASOP, the next hop is determined by node contention mechanism as illustrated above. A malicious node can always use this most aggressive contention mechanism to become the next hop. Once it is included in a route, it can conduct different attacks such as Packet dropping and false misbehaviour.

Packet Dropping

When nodes act as forwarding nodes, offering routes to other destinations, it is expected that such nodes actually forward data packets once the route is setup. However , malicious nodes deviate from this expected behaviour and maliciously drop data packets thereby disrupting transmission. Such Malicious nodes are identified by installing a watchdog and a PathSelector in the Ad-hoc network on every server.

Watchdog

The watchdog identifies misbehaving nodes, while the Pathselector avoids routing packets through these nodes. When a node forwards a packet, the watchdog verifies that the node forwards the packet to all its neighbours. If the node does not forward the packet even to one of its neighbour,then it is misbehaving. The PathSelector uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets.

The watchdog is implemented on every server by maintaining a buffer of neighbours for each and every node. When a node transmits packet to its neighbour,the corresponding entry in the buffer is forgotten by the watchdog, since it has been forwarded on. If an entry for a corresponding node's neighbour has remained in the buffer for longer than a certain timeout, the watchdog increments a failure rate for the node and determines that the node is misbehaving.

Pathselector

Just like the watchdog, the pathselector is run by each server. Each Server maintains a rating for every other node it knows about in the VHR.

Path selector works during the contention scheme. If a node is misbehaving, the watchdog will identify such a node before route discovery itself and assigns a failure rate to such a node. The Pathselector then compares the rating for the nodes that win the contention scheme with this failure rate to determine whether they are misbehaving. If so, they are not included in the route at all. Thus they are avoided from becoming part of the route.

Sybil Attacks

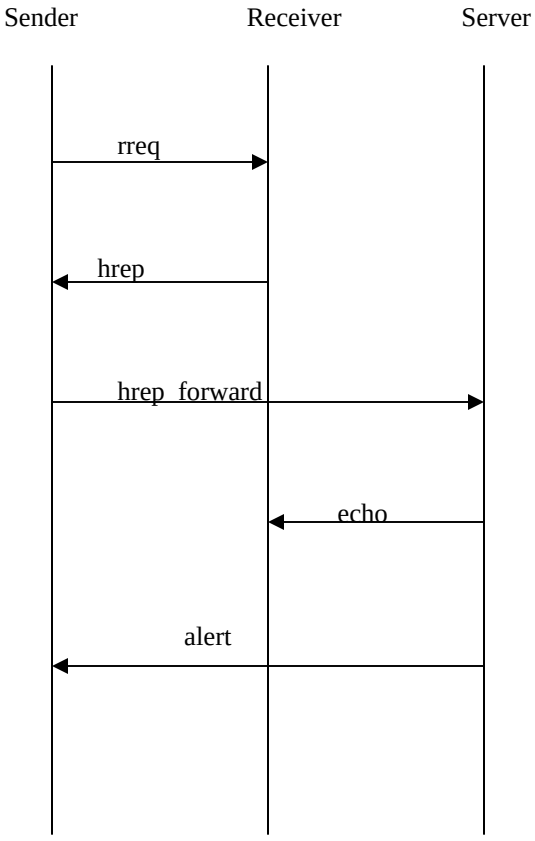
The contention scheme proposed in the AO2P Protocol is vulnerable to malicious nodes that try to become part of the route by claiming False Identities for themselves. Their False Identity is such that, that the malicious node becomes the best choice for data transmission. Such nodes are called as SYBIL NODES.

In order to identify Sybil nodes the following method is proposed.

When a node sends the hrep packet to the sender, the sender forwards the packet to the server for validation. The server then sends a message to the location specified in the Pseudo ID of the hrep packet forward.

If the node responds to it, then the server knows that the node is legitimate and that its positon is geographically correct.

If the node doesnot respond to the message, then the server knows that the node is a Sybil node and that its malicious. Therefore it alerts the sender. The sender then ignores this hrep packet and chooses the next best choice.



Destination Mobility

Once a route is found between the source and the destination, the destination responds to the source by sending the rrep message. There is a possibility that by the time rrep message reaches the source , the destination might have moved to the new location. Hence this when unnoticed can lead to large position errors. In order to keep the source informed about the destination's mobility, the destination keeps sending the alert message to its previous hop telling that it has changed its position and any reference to it for data packet forwarding be informed to the VHR server.

This alert message is forwarded in the reverse path until it reaches the source that initiated the transmission.

The VHR server when intimated will know about the destination's new location and hence the data packets can be sent to the destination properly.

IV. Future Work

We aim to compare the probabilities of a routing discovery failure in the networks where ASOP, AO2P and R-AO2P are used for routing discovery. We also aim to handle those sybil nodes that falsely report other node's IDs as their own IDs .

V . Conclusion

This work proposes a routing algorithm namely ASOP to maintain node anonymity and communication privacy in ad hoc networks. Destination position alone is revealed for routing purposes. Malicious nodes and sybil nodes are handled here. Also, destination mobility is taken care of.

References

[1]. C.E. Perkins and E.M Royer, "Ad hoc On Demand Distance Vector Routing ", Proc. Second IEEE Workshop Mobile Computing Systems and Application,1999

[2]. D Johnson and D.MAltz , " Dynamic Source Routing in Ad Hoc wireless Networks ", proc. ACM SIGCOMM- computer comm. Review ,1996

[3]. C.E. Perkins and P.Bhagawat , "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for mobile Computer", proc. ACM SIGCOMM ,1994

[4] J. Kong and X. Hong, *ANODR:* Anonymous on Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, 4th ACM International symposium on Mobile ad hoc networking and computing, Annapolis, MD, June 2003.

[5]. I. Stojmenovic, "Position Based Routing in Ad Hoc networks ", IEEE comm.. Magazine, vol 40, no 7 , pp 128-134, 2002

[6]. Xiaoxin Wu and Bharat Bhargava," AO2P : Ad hoc On demand Position Based Private Routing Protocol ", IEEE Transactions on Mobile Computing, vol 4, no.4, pp 335-348,2005

[7]. S .Marti , T. Giuli, K.Lai and M.Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", ACM Mobicom, August 2000

[8]. J.Newsome, E.Shi, D.Song, A.Perrig, " The Sybil Attack in Sensor networks – Analysis and defenses ",- 3rd International Symposium on Information Processing in Sensor Networks,2003.

[9] L. Blazevic, L. Buttyan, S. Giordano, J.-P. Hubaux, and J.-Y. Le Boudec, Self-Organization in Mobile Ad hoc networks: *The* Approach of Terminodes, IEEE Personal Communications, pp. 166–174, June, 2000.

Ramya.R is currently doing B.E. computer science and engineering at College of Engineering, Anna University, Chennai, India. Her fields of interest include Networking , Mobile Computing and Operating systems.

Shobana.K is currently doing B.E. computer science and engineering at College of Engineering, Anna University, Chennai, India. Her fields of interest include Networking , Mobile computing and compiler technology.

Thangam.V.S is currently doing B.E. computer science and engineering at College of Engineering, Anna University, Chennai, India. Her fields of interest include Networking, computer architecture and operating systems .

.