ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

An Efficient Secure Routing Protocol in Ad-Hoc Networks

N.Almash Begam[#1], A.Yusuf Khan[*2]

[1#] Department Of Electronics and Communication Engineering,RVS School of Engineering,Dindigul,India.

[2*] Department Of Electronics and Communication Engineering, K.L.N College of Engineering, Madurai, India

ABSTRACT: Anonymous routing schemes in MANETs can be classified into on-demand or reactive routing methods, proactive routing methods and anonymous middleware routing method. A finer classification of reactive routing methods includes hop-by-hop encryption and redundant traffic routing which either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. An Anonymous Location-based Efficient Routing protocol (ALERT) was used to offer high anonymity protection at a low cost. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. To prevent the occurrence of stronger and active attackers, we propose a Secure Cryptographic Based Mix-Zones Routing Protocol (SCMIX).The idea for mix-zones is to prevent the adversary from accessing the content of messages, including the Node's signatures. All legitimate nodes within the mix-zone obtain a symmetric key and utilize this key to encrypt all their messages while within the zone.

KEYWORDS: Anonymity, GPSR, Mix-Zone, Routing protocol, Zone Partition.

I. INTRODUCTION

A Mobile Ad Hoc Networks (MANET) is an autonomous system of mobile nodes. It consists of mobile platforms for example a router with multiple hosts and wireless communications devices. Herein simply referred to as 'nodes' which are free to move. It also may operate in isolation or may have gateways to and interface with fixed network. There are many important research questions in MANET. However, power efficiency is one of the most important issues. It is important to realize that issues such as QoS support, TCP performance, speed of routing repair process and others are secondary if nodes have a high probability of running out of energy resources.

Energy awareness in wireless ad hoc networks actually spans across several communication layers. Advances in battery technology are very slow compared to the results achieved in integrated circuit technology particularly in comparison to the rate of growth in communication speeds. Therefore, saving transmission power represents one of the most significant methods for long term wireless system performance.

II. LITERATURE SURVEY

An Anonymous Location-based Efficient Routing protocol (ALERT) [1] dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

ALARM: Anonymous Location Aided Routing in Suspicious MANETs [2] addresses a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol (ALARM). ALARM uses node‟s current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques (e.g., group

signatures), ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and non-traceability (tracking-resistance). It also offers protection against passive and active insider and outsider attacks. It also offers resistance to certain insider attacks.

Anonymous Geo Forwarding in MANETs through Location Cloaking [3] addresses the problem of destination anonymity for applications in mobile ad hoc networks where geographic information is ready for use in both ad hoc routing and Internet

services and proposes protocols that use the destination position to generate a geographic area called an anonymity zone (AZ). A packet for a destination is delivered to all the nodes in the AZ, which make up the anonymity set. The size of the anonymity set may decrease because nodes are mobile, yet the corresponding anonymity set management is simple. We design techniques to further improve node anonymity and reduce communication overhead.

In [4], Vehicular Networks (VNs) seek to provide, among other applications, safer driving conditions. To do so, vehicles need to periodically broadcast safety messages providing precise position information to nearby vehicles. However, this frequent messaging (e.g., every 100 to 300ms per car) greatly facilitates the tracking of vehicles, as it suffices to eavesdrop the wireless medium. As a result, the driver‟s privacy is at stake. In order to mitigate this threat, while complying with the safety requirements of VNs, we suggest the creation of mix-zones at appropriate places of the VN. We propose to do so with the use of cryptography, and study analytically how the combination of mix-zones into mix-networks brings forth location privacy in VNs. Finally, we show by simulations that the proposed mix system is effective in various scenarios. Our results show that, although the unlinkability of individual mix-zones can be relatively low in some cases, the accumulated unlinkability of the mix-networks is generally very high.

[5] Safety critical applications for recently proposed vehicle to vehicle ad-hoc networks (VANETs) rely on a beacon signal, which poses a threat to privacy since it could allow a vehicle to be tracked. Mix-zones, where vehicles encrypt their transmissions and then change their identifiers, have been proposed as a solution to this problem. In this work, we describe a formal analysis of mix-zones. We model a mix-zone and propose a formal definition of privacy for such a zone. We give a set of necessary conditions for any mix-zone protocol to preserve privacy. We analyze, using the tool ProVerif, a particular proposal for key distribution in mix-zones, and the CMIX protocol.

III. EXISTING METHOD

A. ALERT Routing Algorithm

ALERT uses dynamic Hierarchical Zone Partition. It dynamically partitions a network field into zones and randomly chooses nodes in zone as intermediate relay nodes. This intermediate relay node forms non traceable anonymous route. It uses the GPSR algorithm to send the data to the relay node.

As shown in Figure. 1, the given area is vertically partitioned into two zones X1 and X2. We then horizontally partition zone X1 to Y1 and Y2. After that, we vertically partition zone Y2 into two zones. This type of zone partitioning consecutively splits the smallest zone in an alternating vertical and horizontal manner. This partition process is known as hierarchical zone partition.

ALERT uses the hierarchical zone partition. In each step, it randomly chooses a node in the partitioned zone as an intermediate relay node which is called data forwarder, thus dynamically generating an unpredictable routing path for a message. The zone with k nodes where D exists is called as the destination zone which is denoted as Z_D. k is used to control the degree of anonymity protection for the destination.

In ALERT, each and every data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If both are in same zone, it divides the zone alternatively in the horizontal and vertical directions. This process is repeated until itself and Z_D are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). ALERT aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in Z_D, providing k-anonymity to the destination.

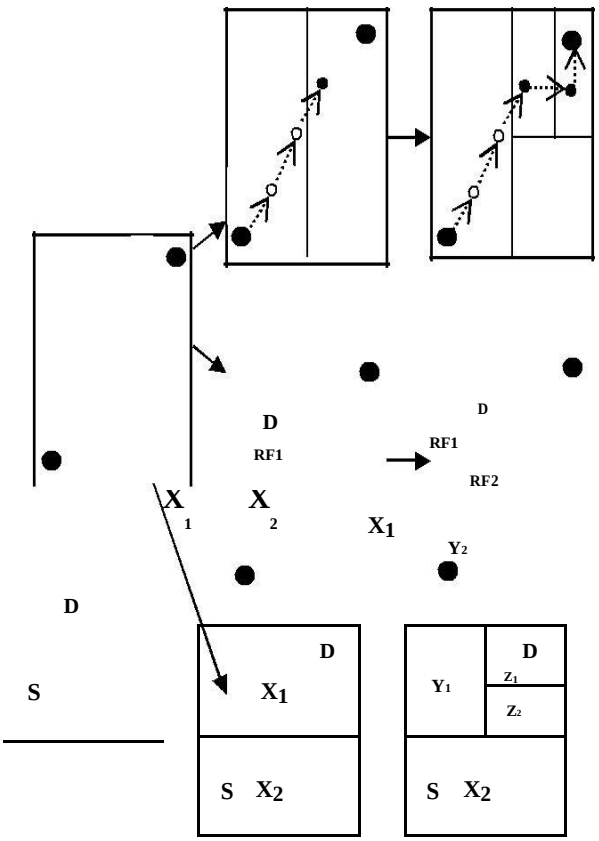


Figure. 1 Hierarchical Zone Partitions

B. Destination Zone Position

We use Z_D rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. There may be problem occur to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D. H is calculated by

$$H = log_2\left(\frac{\rho \cdot G}{k}\right)$$

where G is the size of the entire network area
k is the number of nodes in Z_D
ρ is the node density

C. Source Anonymity

ALERT aims to achieve the anonymity by restricting a node‟s view only to its neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node. To strengthen the anonymity protection of the source nodes, we further propose a lightweight mechanism called “notify and go”. The idea behind “notify and go” is a number of nodes send out packets at the same time as S in order to hide the source packet among many other packets.

“Notify and go” has two phases: “notify” and “go.” In the first “notify” phase, S piggybacks its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and t0. In the “go” phase, S and its neighbors wait for a certain period of randomly chosen time €[t,t+t0] before sending out messages.

S‟s neighbors generate only several bytes of random data just in order to cover the traffic of the source. T should be a small value that does not affect the transmission latency. A long t0 may lead to a long transmission delay while a short t0 may result in interference due to many packets being sent out simultaneously. Thus, t0 should be long enough to minimize interference and balance out the delay between S and S‟s farthest neighbor in order to prevent any intruder from discriminating S.

D. Strategies against Attacks

ALERT has strategies to effectively counter intersection and timing attacks.

1) Timing Attacks

In timing attacks, an intruder can identify the packets transmitted between S and D through packet departure and arrival times. From this observation, the attacker can detect S and D. For example, two nodes A and B communicate with each other at an interval of 4 seconds. After a long observation time, the intruder finds that A‟s packet sending time and B‟s packet receiving time have a fixed five second difference such as (16:00:56, 16:01:00) and (12:08:33, 12:08:37). Then, the intruder would guess that A and B are communicating with each other. Avoiding the exhibition of interaction between

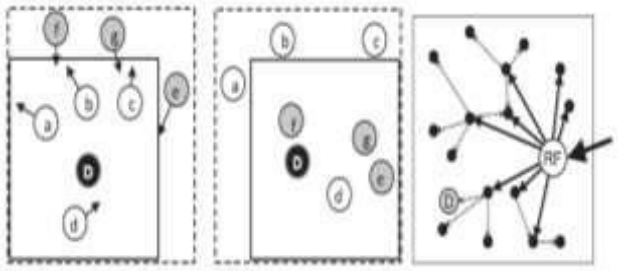
communication nodes is a way to counter timing attacks.

In ALERT, the "notify and go" mechanism and the broadcasting in Z_D both put the interaction between S-D into two sets of nodes to obfuscate intruders. Also, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly. This again keeps an intruder from identifying the S and D.

2) Counter Intersection Attacks

In an intersection attack, an attacker may have the information about active users at a given time through repeated observations. The attacker with this information can determine the sources and destinations that communicate with each other. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in Z_D during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the
destination zone except D. As a result, D is identified as the destination because it always appears in the destination zone.

Figure. 2. a). is the status of a Z_D after a packet is broadcasted to the zone. The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in Z_D. Figure. 2. b) is the subsequent status of the zone the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g, and D are in Z_D. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node.



a) b) c)

Figure. 2 Intersection Attack and Solution

To counter the intersection attack, ZAP dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. However, the former strategy increases the communication overhead, while the latter may not be suitable for long duration communication. Instead of adopting such a mitigating mechanism, we propose another strategy to resolve this problem. Note that the attacker can be puzzled and lose the cumulated observation by making it occasionally fail to observe D"s reception of packets. Since packets are delivered to Z_D constantly in long-duration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packet pkt1 to a partial set of nodes, say m nodes out of the total k nodes in the zone. The m nodes hold the packets until the arrival of the next packet pkt2. Upon the arrival of the next packet, the m nodes conduct one-hop broadcasting to enable other nodes in the zone to also receive the packet in order to hide D.

Figure. 2. c) shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt1 and pkt2 are mixed, an attacker observes that D is not in the recipient set of pkt1 though D receives pkt1 in the delivery time of pkt2. Therefore, the attacker would think that D is not the recipient of every packet in Z_D in the transmission session, thus foiling the intersection attack.

IV. PROPOSED METHOD

Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. Also, ALERT cannot be applied to all network models. ALERT can be applied to Random Way Point model and Group Mobility Model. To
prevent the occurrence of stronger and active attackers, we propose a Secure Cryptographic Based Mix-Zones Routing Protocol (SCMIX).

An unobserved zone functions as a mix zone where the mobile nodes change pseudonym and mix with each other. Note that the Mobile nodes do not know where the mix zone is (this depends on where the adversary installs observation spots).

We propose to create mix-zones at predetermined locations and to force pseudonym changes to take place within those regions. Since the location of mix-zone is fixed, the adversary can identify them and thus could easily attempt to eavesdrop transmissions originating in the mix-zone area. The adversary observes the timing and the location of the entering and exiting node in order to derive a probability distribution over the possible mappings. To solve this problem the timing of events depends on the delay characteristics of the intersection structure. Likewise, the location of entering and exiting

nodes depends on their trajectory in an intersection.

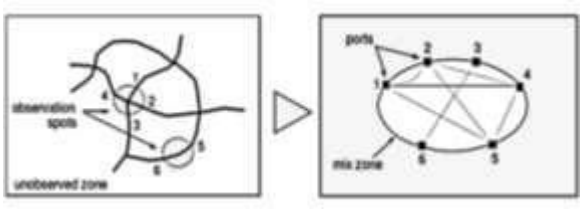


Figure. 3 Mix-Zone Concepts

The idea for mix-zones is to prevent the adversary from accessing the content of messages, including the Node's signatures. All legitimate nodes within the mix-zone obtain a symmetric key and utilize this key to encrypt all their messages while within the zone. We improve location privacy of mix-zones via extensions to the SCMIX protocol. SCMIX Protocol distributes Keys for encrypting beacon messages while in the mix-zone.

While the mobile node is inside of the cryptographic mix zone, all communication is encrypted and therefore an adversary cannot read-out useful information (including meta-information) from its messages. Nodes in the mix-zone forward the symmetric key to Mobile nodes that are in direct transmission range outside of the mix zone such that these nodes are also able to decrypt messages. Mobile Nodes then change pseudonyms while being inside of the mix-zone.

V.**CONCLUSION**

The concept of mix zone refers to a service restricted area where mobile users can change their pseudonyms so that the mapping between their old pseudonyms and new pseudonyms are not revealed. Since the location of mix-zones is fixed, the adversary can identify them and thus could easily attempt to eavesdrop transmissions originating in the mix-zone area. To solve this problem, we propose a Secure Cryptographic Based Mix-Zones Routing Protocol (SCMIX). In our future work, we intend to study how the frequency of the pseudonym change influences the level of privacy achieved**.**

REFERENCE

[1] Zhi Z. and Choong Y. K. (2005), „Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy", Proc. Third Int"l Workshop Mobile Distributed Computing (ICDCSW).

[2] Defrawy K. E. and Tsudik G. (2007), „ALARM: Anonymous Location- Aided Routing in Suspicious MANETs", Proc. IEEE Int"l Conf. Network Protocols (ICNP).

[3] Wu X., Liu J., Hong X. and Bertino E. (2008), „Anonymous Geo-Forwarding in MANETs through Location Cloaking", IEEE Trans. Parallel and Distributed Systems, Vol. 19, No. 10, pp. 1297-1309.

[4] Freudiger J., Raya M., Felegyhazi M., Papadimitratos P. and Hubaux J. (2007), „Mix-zones for location privacy in vehicular networks", Proc. First Int"l Workshop onWireless Networking for ITS IntelligentTransportation Systems (WiN - ITS"07).

[5] Dahl M., Delaune S. and Steel G. (2010), „Formal analysis of privacy for vehicular mix-zones", Proc. of the 15th European conference onResearch in computer security (ESORICS"10), pp. 55–70.