CACS : Closed Anonymous Communication System for MANETs

G V Eswara Rao
Department of Computer Science & Engineering
Vignan's Institute Of Engineering For Women , Visakhapatnam, AP, 530 046, India

D. Kamal Kumari
Department of Computer Science & Engineering
Vignan's Institute Of Engineering For Women , Visakhapatnam, AP, 530 046, India

N. Krishna Santosh
Department of Computer Science & Engineering
Vignan's Institute Of Engineering For Women , Visakhapatnam, AP, 530 046, India

Abstract - In hostile environments, communication anonymity has to be preserved to ensure security. Network members should not reveal their real identities to others but use pseudonyms (identity-free). Their locations also need to be concealed to protect themselves (location anonymity). The source and destination of a flow should be indistinguishable among all the nodes (source/destination anonymity) and their end-to-end relation should be hidden (end-to-end communication relation anonymity). A flow must be untraceable, should not be discovered by malicious adversaries (route anonymity). All these strict requirements become the heavy tasks of anonymous routing protocols. Previously proposed anonymous routing schemes have provided anonymity for MANET communications on certain levels, but they all suffer from different defects. The most common drawback is that they sacrifice the networking performance. Normally, a routing protocol has the route discovery phase and the message transfer phase. During the second phase, most of the prior schemes require the packets to be encrypted and decrypted at each node in the path. These cryptographic operations incur large cost. All the existing schemes suffer from the lack of universal applicability, the conflict with secure routing, and the lack of differentiated anonymity provision.

Keywords – privacy, mixed nodes ,anonymity, security.

I. INTRODUCTION

During the last two decades, research in various aspects of mobile adhoc networks (MANETS) has been very active, motivated mainly by military, disaster relief, and law enforcement scenarios. More recently, location information has become increasingly available through small and inexpensive GPS receivers, partially prompted by the trend of introducing location-sensing capabilities into personal handheld devices[1]. A natural evolutionary step is to adopt such location-based operation to MANETS. This results in what we term location-based MANETS. In such a MANET, devices rely on location information in their operation. The main distinguishing feature of the envisaged location-based MANET environment is the communication paradigm, based not on permanent or semi-permanent identities, addresses or pseudonyms, but on instantaneous node location. In other words, a node(A) decides to communicate to another node(B), depending on exactly where (B) is located at present. If node location information is sufficiently granular, a physical MANET map can be constructed and node locations instead of persistent node identities can be used in place of network addresses. In some applications, such as military, law enforcement and search-and-rescue, node identities are not nearly as useful as node locations. Such critical settings have certain characteristics in common. First, node location is very important knowledge of the physical, as opposed to logical or relative topology, enables avoiding wasteful communication and focussing on nodes located within a specific area. Second, critical settings must contend with security and privacy attacks. Security attacks might attempt to distribute false or impede propagation of genuine routing information. Whereas, privacy attacks aim to track nodes as they move.

In this paper, we consider what it takes to provide privacy-preserving secure communication in hostile and suspicious MANETS. We introduce some mix modes into MANET networking, for Anonymous Location-Aided Routing in MANETS (ALARm) that demonstrates the feasibility of simultaneously obtaining, strong privacy, and security properties, with reasonable efficiency. In this context, privacy means node anonymity and resistance to tracking. Whereas, security includes node/origin authentication and location integrity. Although it might seem that our security and privacy properties contradict each other, we show that some advanced Mix Agent Algorithms can be used to reconcile them.

The main challenge arises from the need to reconcile security and privacy anonymity and untraceability requirements that we address below. Based on the above discussion, we consider link-state to be best-suited for supporting location-based routing with the privacy and security features described earlier. In the rest of this paper, we use a simple flooding based scheme to illustrate the operation of Mix nodes. However, we note that any optimization for reducing LS flooding overhead (e.g., MPR-based flooding in OLSR), can be easily integrated into Mix nodes.

Our main contributions in this paper are as follows:

- *Privacy*: There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations (movement patterns) cannot be linked.
- *Security*: The network must be resistant to passive and active attacks stemming from both outsiders and malicious(e.g., compromised) insiders.
- *Performance*: Security and privacy goals must be achieved without undue sacrifices in performances (i.e., without requiring excessive computations and/or high delay).

II. Related Work

Secure MANET routing has been extensively studied in both security and networking research communities. A comprehensive survey of this work can be found in [2]. Prominent secure on-demand MANET routing protocols include SRDP[30], Ariadne[3], and SEAD[4]. All of them focus on securing route discovery, route maintenance and defending against modification and fabrication of routing information. Privacy, especially, tracking-resistance, is not one of the goals of these protocols. A more relevant body of research focussed on proactive anonymous MANET routing protocols, such as SPM[5]. SPM is a modified link-state protocol that requires nodes joining (and leaving) the MANET to report such events to "super" nodes. Super nodes collect and distribute topology information and also handle communication between different "local" MANETS. SPM assumes that nodes periodically change their pseudonyms and that they communicate based on instantaneous pseudonyms. SPM is thus identity-based and requires nodes to be able to retrieve each other's public keys. Another related research direction tackles anonymous on-demand MANET routing, eg., D-ANODR[6].

In parallel to our work on ALARM [7], [5] proposed using group signatures to construct pseudonyms in vehicular adhoc networks (VANETs). ALARM is designed for more general MANET settings (VANETs are a special type of MANETs) and takes into account active and passive insider attacks..

III. Mix Agent Algorithms

Mix Nodes in Mixed network:

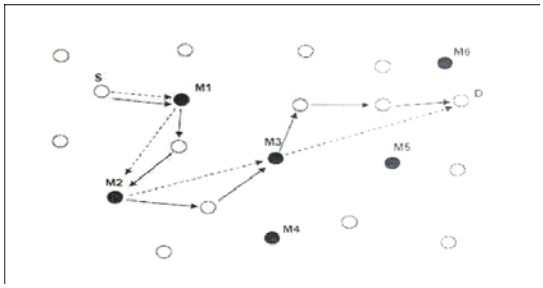

Figure 1. A mixed-net example in a wireless ad hoc network

In this section, our enhanced mix route algorithm is presented which is called *MixRoute.* The purpose of MixRoute is to find mix routes for an end-to-end connection. Several design goals are set for the algorithm. First, connection anonymity should not be violated during the mix route discovery process. Second, the algorithm should find a short mix route based on the current network topology. As the network topology changes, the algorithm should update the mix route. Third, the algorithm should have low and bounded overhead. First the algorithm is described, followed by a detailed discussion. MixRoute consists of two independent processes: mix advertisement (using MADV messages), and mix route discovery and update (using DREG, RREQ and RUPD messages). It should be emphasized that the " mix route discovery" process runs on top of any underlying routing protocol. In essence, the mix route discovery process finds routes consisting of "virtual links" between mix nodes - a virtual link in the mix-net is a path in the physical network.

- The purpose of mix advertisements is for the mix nodes to announce their presence to non-mix nodes. Each non-mix node tries to pick the closest mix node as its first mix node on the route - the closest mix node serves a function in anonymous routing as seen below.

- Due to node mobility, each non-mix node may dynamically change the mix node chosen as its nearest mix node. To make each mix node aware of its nearest mix node relationship with non-mix nodes, the non-mix nodes use DREG messages to register at their nearest mix nodes.

- In this approach, when a node *S* needs to find an anonymous route (through one or more mix nodes), it sends a RREQ message to the destination *D* via a custom mix route formed by a set of randomly chosen mixes or by S's closest mix node. The custom mix route may not be the right choice from performance perspective, therefore, the rest of the mix route discovery process attempts to find a better mix route for the connection. For instance, if *S* chooses a mix *Ma* randomly, then the mix route for the RREQ will be *S -> M_3 ~* D.* The RREQ packet is routed from *S* to *M3* using the underlying routing protocols (we have chosen DSR [8]). and from *Ms* to *D* similarly. When *D* receives the RREQ, the destination node realizes that it is an endpoint for an active connection. Therefore, it registers with its closest mix node by sending a DREG message.

- Any mix node that has a non-empty list of registered non-mix nodes periodically transmits a RUPD message as elaborated later. The purpose of RUPD transmissions is to allow a source node to discover a mix route regarding a particular destination node (A RUPD message contains a list of all destination nodes currently registered at the mix node who creates the message).

  In the rest of this section there will be further elaborations on the above discussed algorithm.

Algorithm 1: Mix Advertisement algorithm for non- mix nodes to find the closest mix:

---

1. Every mix periodically broadcasts mix advertisement (MADV) messages to announce its presence to non-mix nodes in the neighbourhood. The time interval between two consecutive advertisements is ADVERTISEJNTERVAL. MADV from mix *M* has message format:
   (MADV, M —> ALL, seqnum, radius)
   where (i) seqnum together with *M's* address uniquely identify a MADV message,
   (ii) The *radius* value indicates how far the message has propagated. When the message is created, it is set to 0.

2. A non-mix node learns mixes in its neighbourhood from received MADV messages and maintains the closest mix information, which is also the node's closest mix. As time passes, the node's neighbourhood may change. Therefore, a non-mix node's closest mix is not constant. It is also possible that a non-mix node loses connectivity with its current closest mix. So if a non-mix node does not receive MADV packets from the current closest mix for

   (i) Time interval of length =
   2*ADVERTISEMENT INTERVAL.
   it switches to a new closest mix. A non-mix node only retransmits MADV messages from its closest mix. Every time when a MADV message is retransmitted,

(ii)the *radius* value in it is incremented by1

3. A mix node discards MADV messages that it receives.

The described algorithm is unlike the conventional, network-wide flooding algorithm. Each MADV message has a limited flooded area. Typically, it only arrives at nodes that are closer

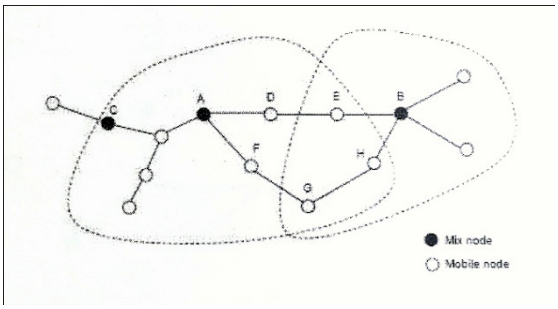

Figure 2. Flooded area of mix advertisement

to it than to any other mixes. An example is used to illustrate this idea. In Figure 2. the border of two mixes' flooded area is shown by dashed line. *A* is the closest mix to *D.* So *D* will retransmit *A's* MADV messages. But *E* does not retransmit .A's MADV's it received from *D* because mix *B* is closer to it than *A* is. The validity of this algorithm can be shown by considering a non-mix node that receives two MADV messages, one from the closest mix *M,* another from a farther mix *X.* The *radius* values in the two messages must satisfy *radius(M) < radius(X).* Suppose that the node retransmits both messages: A neighbouring node that receives the two messages will find that the above relationship still holds because the *radius* values in both messages are increased by 1, respectively. In other words, based on these two messages, *X* can never be closer to any downstream nodes than *M* is. So it is unnecessary to forward the MADV messages from *X.*

Algorithm 2: Mix Route algorithm for Route Discovery and Update :

1. *RREQ phase: 3* assembles a RREQ message and sends it to *D* via a custom mix route. As we mentioned, a custom mix route can be a random route consisting of randomly chosen mixes, or be the closest mix of *S* as in this example. The RREQ message is a uni-cast message.

   So *S* can encrypt the content of the message with D's public key to prevent tracing of the message by an attacker. The RREQ packet may be lost during transmission. So a timcout-based retransmission mechanism must be activated by *S.*
2. *DREG phase:* When *D* receives a RREQ message, it knows that it is destination of a new end-to-end connection. If *D* did not yet register at its closest mix *(Ms* in this example), it does so by sending a Destination Registration (DREG) message to the mix. Let *M* be U's closest mix. The DREG message would have format

(DREG, D- M, seqnum)*

D must send DREG messages periodically to maintain its association with the mix. There are several reasons for this design. First, DREG messages may be lost during transmission and never reaches the mix. Second, as network topology changes, *D* may switch to a different closest mix. In this case, *D* simply sends DREG messages to the new closest mix and increases the *seqnum* in it. The old closest mix may learn this change from one of two events. One is expiration of *D's* registration record because there is no new DREG message arriving from *D.* Let DREG JNTERVAL be the time interval between two consecutive DREG messages. The expiration time of a destination node's registration at mix is set as

2 * DREG INTERVAL in the algorithm. Another is receiving RUPD messages from D's new closest mix (explained below).

3. *RUPD phase:* Every mix maintains a list of registered destination nodes. If the list is not empty, it periodically broadcasts RUPD messages. The time interval between two consecutive broadcasts is RUPD-JNTERVAL. RUPD message from a mix *M* is of the format

(RUPD, M -» ALL, seqnum, I, path)

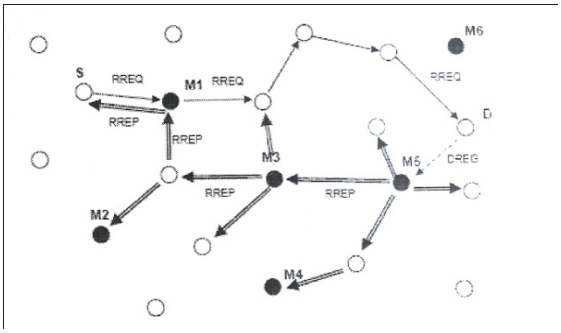

Figure 3. Mix Route Discovery Process

where

(i) *seqnum* together with M's address uniquely identify a RUPD message,
(ii) is the list of destination nodes currently registered at *M.* Each entry of the list includes node address and the latest DREG *seqnum*
(iii) *path* records a mix route that the packet has traversed during flooding. Initially, *path* contains M, the initiator of the message.

The flooding of a RUPD message proceeds as follows. The initiator mix broadcasts the message locally. If a node *X* that receives the RUPD message has pending data packets in its queue addressed to destination node(s) in /, then it copies the mix route in *path* and uses the reverse mix route in delivering those data packets[1]. If *X* is a mix, then it checks whether any destination node in *I* carries a higher DREG *seqnum* and updates its own list. When the above processing is completed, *X* retransmits the RUPD message, and if A' is a mix, it appends its ID to the *path* before retransmitting.

It is possible that *X* receives the same RUPD message for multiple times. To ensure that a RUPD message is retransmitted only once, *X* keeps a record of each RUPD message it retransmitted. However, from the multiple RUPD messages that arrive via different paths, *X* may obtain multiple distinct mix routes to the same destination node. In Figure 3, the retransmissions of RUPD message are indicated by double arrows. It is shown that *S* will find a mix route

Mi —* M3 —* *M5* for its connection to *D.*

From the above description, we know that the RUPD message is flooded along the shortest path tree rooted at the initiator mix. For the same destination node, different source nodes receive different mix routes and the minimum length of each mix is 1. The idea is that each mix caches the mix routes it received and broadcasts them along with MADV messages. The source node of a connection will use the mix Route received from its closest mix node, which contains at least two mixes.

1. The update of mix route for an anonymous connection is realized by periodically RUPD broadcasts. If a node is not destination of any active connection, it should stop sending DREG messages to its closest mix node. It is assumed that an in-band protocol exists for the source node to inform the destination node of connection termination.

IV. EXPERIMENTAL RESULTS

We conduct a simulation study on the proposed system in terms of Routing load, Packet-Delivery –Fraction, Average End-End-Delay, Control packets rate along with mixed nodes pause time. These are the metrics for evaluating the solution to anonymize communication end-end points .

We implemented our model using the NS2 simulator for modelling the AODV protocol and the AODV with mixed network independently. We tested in simulated environment which gives the approximate results as the real time environment. We have used a well defines NS2 simulator in Linux environment on 2.4 GHz processor and 2GB primary memory computer.

The below figure (i.e Figure 4) shows the relation between the route load and packet delivery fraction (pdf) along with the network pause time used in the AODV(without mixed network) testing.

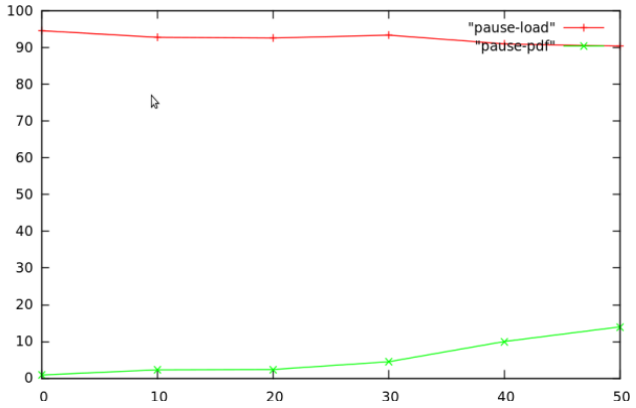

Figure 4. Load and Pdf VS pause-time

The below figure (i.e Figure 5) shows the relation between the route load and packet delivery fraction along with the proposed network pause time used in the AODV (with mixed network) testing.

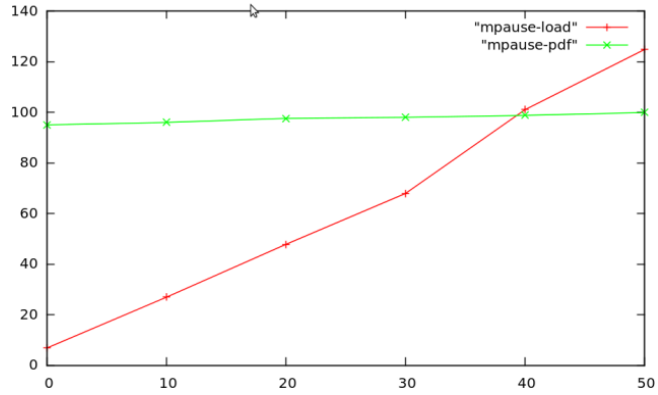

Figure 5. Route load and Pdf VS pause-time

V. CONCLUSION AND FUTURE WORK

This paper presented the CACS system, which supports anonymous location-based routing in suspicious MANETS. CACS system relies on group signatures to construct one-time pseudonyms used to identify nodes at their present locations. The protocol works with any group signature scheme and any location-based forwarding mechanism from our simulation study, it is clear that the proposed Mix Agent algorithms (Mix Advertisement and Mix Route Discovery) performs well, in terms of its gives a comprehensive solution to anonymize communication end-points, keep the location and identifier of a node unlinkable, and reduce traffic overhead. Much report have been made to reduce transmission overhead routing.

In future, the work can be extended by aiming to improve the simulation area, number of mixed nodes and mixed node speed, and This Simulation used to compare the proposed algorithm to the static mixed-net model to show the improvements.

REFERENCES

[1] Nokia 6110 Navigator, http://europe.nokia.com/A4344146,2011.
[2] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad HocRouting," IEEE Security and Privacy, vol. 2, no. 3, pp. 28-39, 2004.
[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, nos. 1/2, pp. 21-38,2005.
[4] J. Kim and G. Tsudik, "SRDP: Securing Route Discovery in DSR," Proc. Mobiquitous, 2005.
[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. Fourth IEEE Worksho Mobile Computing Systems and Applications, pp. 3-13,2002.
[6] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous on Demand Routing for Mobile Ad Hoc Networks,"roc SECURECOMM, vol. 28, pp. 1-10, Sept.2006.
[7] J. Ren, Y. Li, and T. Li, "SPM: Source Privacy for Mobile Ad HocNetworks,"EURASIP J.Wireless Comm. Networks, vol. 2010,p.5,2010.
[8] K.E l Defrawy and G. Tsudik,"ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP '07), pp. 304-313, Oct. 2007.