

# A New Approach for Routing in Adhoc Network

S. Sridevi<sup>1</sup>, C. Swaraj Paul<sup>2</sup>, R. Balakrishna<sup>3</sup>

Assistant Professor, Department of CSE, Vels University, Chennai, Tamil Nadu, India<sup>1</sup>

Assistant Professor, Department of CSE, Vels University, Chennai, Tamil Nadu, India<sup>2</sup>

Teaching Assistant, Department of CSE, Vels University, Chennai, Tamil Nadu, India<sup>3</sup>

**ABSTRACT:** Privacy and anonymity are critical security issues to many large-scale MANET applications such as military communication networks. These applications are more likely deploying the networks heterogeneously and hierarchically due to administrative needs or routing efficiency. When the size of the network scales up, the routing overhead incurred by existing flat anonymous routing protocols increases fast as the required number of public key operations increases, thus resulting in deteriorated routing and data communication performance. In this paper, we introduce a novel hierarchical anonymous on-demand routing protocol tackling this limitation. In addition to guaranteeing routing and data delivering security, the scheme provides two levels of anonymity: intra-group and inter-group. By exploiting the hierarchical network structure, it effectively controls computational overhead while preserving anonymity, hence accommodates to larger-scale MANETs.

**KEYWORDS:** Anonymity, Protocols, Manets.

## I. INTRODUCTION

Instant communication support using mobile ad hoc networks (MANETs) in applications often demands that networks operate in a large scale. Examples of such applications include auto-mated battlefield support, disaster relief, and vehicular networks, etc.. Such networks will be heterogeneous and hierarchically organized due to administrative needs or for routing efficiency. Many routing protocols have been proposed as scalable solutions for large-scale scenarios. These protocols use different mechanisms to achieve routing efficiency, including: clustering mechanisms (HSR [1] and Hi-TORA [2]), geographical information (GPSR [3]), dynamic addressing (DART [4]), grouped motion behavior (LANMAR [5]), proactive hierarchical routing (HOLSR [6]), or a hybrid of proactive and on-demand update strategies (ZRP [7], HARP [8] and SAFARI [9]). Many of MANET applications also take network privacy and anonymity as a critical security requirement in order to protect the operation against the security vulnerability of wireless media. A number of anonymous MANET routing protocols have been proposed in recent years. These protocols include ANODR [10], ANONDSR [11], ASR [12], MASK [13] and SDAR [14]. They achieve anonymity goals such as identity anonymity and unlink ability in routing, as well as anonymous data delivery by using various security mechanisms. Typically these protocols use public key cryptography more or less in the route discovery phase. For resource-constrained mobile devices, the public-key operations could result in long route acquisition delay and degrade packet delivery ratio [15] [16]. When the size of the network scales up, the lengths of end-to-end paths grow accordingly on average. This will incur prohibitive computation and communication overhead along a long path. In addition, a long path tends to break more frequently in a mobile network, resulting in frequent maintenance and re-discovery processes. All these greatly deteriorate communication efficiency and network performance.

## II. RELATED WORK AND MOTIVATION

# International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 6, September 2015

A number of anonymous routing protocols have been proposed such as ANODR [10], ANONDSR [11], ASR[12], MASK [13] and SDAR [14]. They are all on-demand protocols but use different approaches for anonymous routing. ANODR and ASR use a boomerang type onion, a layered cryptographic structure on which appending and peeling off are performed by the same forwarding nodes. ANONDSR and SDAR use a suggestion box cryptographic structure, i.e., each node appends a cryptographic layer, and the destination peels off all the layers and reconstructs a new onion for return path. MASK and SDAR use periodic hello messages to establish pair wise trust relationship between neighbors. MASK then uses the trust and pseudonyms for route discovery.

Cryptographic tools are important in order to achieve security and privacy in data communications. In these protocols, public key cryptography is used at different stages in routing operations. Usually, public key cryptography uses more CPU time than symmetric key cryptography. For resource-constraint mobile devices, the computation time could be very long. Some measurements on Intel Strong ARM 200MHz CPU based Pocket PC running Linux are presented in [17]. Based on the measurements, if a payload is of 512 Bytes, ECC uses 1209ms/637ms for encryption/decryption respectively, while AES uses 140 $\mu$ s for encryption/decryption. During the route discovery, ANODR and ASR perform asymmetric encryption/decryption primarily in RREP forwarding stage at each hop. ANONDSR and SDAR, instead, perform asymmetric encryption/decryption in RREQ flooding stage at each hop. In addition, ANONDSR and SDAR perform both public key and symmetric key operations at the destination nodes. Assume the path length of a discovered route is  $L$ , the computational overhead for discovering the route is  $OH_{\text{asymmetric}} \cdot L$  for ANODR and ASR, and  $2 \cdot OH_{\text{asymmetric}} \cdot L$  for SDAR and ANONDSR, where  $OH_{\text{asymmetric}}$  is the computation latency of using public key cryptography. When message size is taking into consideration, the overhead will increase if a message needs to be processed in several blocks. We then draw our attention to the usage of the public key cryptography when evaluating existing routing protocols and designing new protocols.

Apparently when the network scales up to a certain extent, the flat anonymous routing schemes will incur very long route acquisition latency. In a mobile network, such initial latency in data communication will result in low data delivery ratio, since a discovered path may have broken at the time data is transferred. In [18], a location privacy framework for wireless networks with infrastructure is proposed which bears the flavor of a hierarchical scheme. For achieving unlinkable communication an anonymous bulletin board is introduced as a means of rendezvous. This approach requires the nodes in the network to check the bulletin board periodically to see if there are call-back requests from potential communication counterparts. In case of a multi-hop network attaching to a base station, an aforementioned anonymous routing is suggested. In the framework, the infrastructure is used as the upper level but no ad hoc routing is needed. This differs from HANOR in which a fully mobile ad-hoc network is targeted.

## III. SYSTEM MODEL

### A. Network Scenarios

The hierarchical mobile ad-hoc network scenario we base this research on has two logical tiers. The lower tier is a network of multi-hop clusters and the high lever is a network of cluster headers (referred as groups and group leaders in the rest of the papers). Such network architecture can be pre-configured by network administrators or fully self-configured. When high-bandwidth backbone networks are possible, gateways in each group will interconnect group leaders. When no physical hierarchy exists, we assume a multi-hop clustering algorithm to form groups and elect leaders. Communication between two group leaders (a virtual link) needs to be relayed by other wireless nodes. Obviously, when groups can be pre-configured and/or physical support is feasible, we expect better performance. So at times, we will include such discussions.

In HANOR, we assume a distributed certificate authority(CA) infrastructure. The CA is responsible for assigning (and thus possessing) the public keys and private keys of all nodes before they join the network. For each group(elected or pre-configured), a pair of asymmetric keys, denoted as  $(PK_g, SK_g)$  are assigned. The group ID is derived from  $PK_g$  by the group leader, and distributed to the group members securely. The way the group ID is generated ensures that the group's public key is kept secret from group members. For data

# International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 6, September 2015

communication, we assume that each source-destination pair shares a global trapdoor, as been widely used in existing anonymous routing protocols such as SDAR, ANODR, ASR and ANONDSR.

## B. Adversary and attack model

Adversaries can be categorized according to their behaviors: passive eavesdroppers and active attackers; or according to their knowledge about the network: external attackers and intruders; or according to their communication ability: individual or collaborative attackers. The HANOR protocol is mainly designed to deal with passive attacks, their goals are to get privacy information without disrupting routing operation. The adversaries could simply eavesdrop, or act protocol-compliantly when they are intruders. But we assume adversary's computational power and capabilities of node intrusion are limited. Multiple attackers can communicate to integrate their knowledge about the network. However, we don't assume a global adversary who is able to monitor all of the wireless transmissions. Such an attack could be either impractical to launch or be very expensive when network is large.

## III. HIERARCHICAL ANONYMOUS ROUTING PROTOCOL

### A. The Scheme Overview

HANOR accomplishes the following anonymous goals:

- Establishing a path anonymously. This achieves anonymous goal in the route discovery process.
- Transmitting data anonymously. This accomplishes anonymous goal in data forwarding process.

Anonymous route discovery of HANOR is conducted in a hierarchical way, consisting of intra-group anonymous routing and inter-group anonymous routing. The intra-group anonymous routing includes two phases: (1) route discovery within the source group, where the source node tries to establish an anonymous route towards the group leader, and (2) route discovery within the destination group, where the destination group leader establishes an anonymous route towards the destination. The inter-group anonymous routing phase will establish an anonymous route from the source group leader to the destination group leader. Thus, in a typical scenario where the source and destination reside in different groups, the routing process follows the following three consecutive phases: in the source group, between groups and in the destination group. We adopt ANODR [10] for intra-group anonymous routing. A few modifications to ANODR protocol are needed so it can be integrated with the inter-group protocol.

These modifications are presented throughout the following subsections. On the other hand, route discovery in the source group could wait long before completion due to the fact that the RREQ and RREP procedures are separated by the inter-group routing and intra destination group routing. This could result in negative influence on the successfulness of the route discovery. The problem can be solved in several ways. We will discuss these alternatives in the discussion subsection.

In designing the inter-group routing, we intend to treat each intermediate group as a single anonymous routing unit. Such design enables us to retain the cryptographic operation at the group level, which greatly reduces the end-end route acquisition delay. The inter-group routing will establish an one-way relation between groups and keep the cryptographic operation inside the group efficient.

D

A

# International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 6, September 2015

Fig. 1. HANOR Route Discovery

Figure 1 illustrates the process of the route discovery for a cross group path. A route is discovered from the source node  $S$  to the destination  $D$ .  $LS$  and  $LD$  are the group leaders of the source and destination groups respectively. The routing process consists of three phases. When  $S$  wants to discover a route to  $D$ , it constructs a route request (RREQ) message and sends it to  $LS$  using local in-group anonymous routing algorithm (adapted ANODR is used for this purpose). According to the RREQ,  $LS$  assembles an inter-group route request message (GRREQ) and send it to all other group leaders in the network. Inter-group routing scheme is used in this stage. Each group leader receiving GRREQ messages tries to find whether the destination is one of its members. It again uses flat anonymous routing algorithm (adapted ANODR) to establish a route to the real destination  $D$ , which sends back a route reply (RREP) message to  $LD$ .  $LD$  continues to reply with a GRREP message to  $LS$ , which after receiving GRREP sends RREP to the original source node  $S$ . If the original path between  $S$  and  $LS$  has been broken due to node mobility,  $LS$  can initiate a reverse route request trying to proactively find a route from itself to  $S$ . After the sub-route between  $S$  and  $LS$  is discovered, an anonymous route has been established from  $S$  to  $D$ .

## B. Anonymous Route Request

Anonymous Route Request in the source group: The anonymous route request starts with intra-group routing in the source group. We utilize ANODR to establish an anonymous route from the source node to the source group leader ( $LS$ ). The original ANODR RREQ message is modified to include two functions: RREQ flood control and informing  $LS$  the destination trapdoor. In addition, considering the fact that  $LS$  will be used by its group members when they initiate a communication, we avoid any direct use of  $LS$ 's trapdoor so to prevent the content correlation attack. The modified RREQ message looks like: The propagation of GRREQ messages is a controlled flooding by  $H^{nr}$  ( $GID_c$ ), similar to the previous RREQ flooding control, together with the sequence number, i.e., only nodes within the group who receive a GRREQ with a new seq2 will rebroadcast it.

<sup>1</sup> The field  $H^{nr}$  ( $GID$ ) is used to control the RREQ flooding to be within the group (here, the source group).  $H_1$  is a parameterized one-way hash function for each specific group and it is updated after each election process or periodically. Thus, before forwarding a RREQ, each node (including the leader) chooses a random number  $n_r$  (bounded by a maximum value) and applies  $H_1$  on its group ID  $GID$  for  $n_r$  times. Upon receiving an unseen RREQ message (a new seq1), a node applies  $H_1$  a threshold number of times on  $GID$  and compares the results with the fifth field of the received RREQ, i.e.,  $H^{nr}$  ( $GID$ ). If there is a match, the RREQ message is from a node of the same group, and it will be forwarded with an updated  $n_1$ . Otherwise, the RREQ is discarded. Clearly, no real group IDs will be revealed in the route request messages and the flooding is controlled. The trade-off is the computation time for one way hash function, which can be ignored compared to public cryptosystems.

The last field is encrypted by the public key  $PK_{LS}$  of the  $LS$ . It serves as a trapdoor of the  $LS$ , since it is the only node that is going to and is able to decrypt it. And it also prevents correlations among multiple RREQs sending to the same  $LS$ . The encrypted form also protects the source tag  $Src$ , the trapdoor for the destination  $trdest$ , and an one-time key  $TK$  to be used in the RREP procedure. After all, the leader of the source group will receive the RREQ message.

Inter-Group Anonymous Route Request: The source group leader  $LS$  initiates the inter-group routing phase by sending an inter-group route request message (GRREQ) to all other group leaders in the network. Each group leader receiving the GRREQ message tries to find the destination in its group. Thus, after  $LS$  receives the RREQ message, it stores seq1,  $TK$  and  $Src$ , picks up a new sequence number seq2, and assembles and floods a new inter-group GRREQ message using the  $trdest$ . The seq2 will uniquely identify this inter-group

# International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 6, September 2015

route discovery and it is recorded with the tuple  $\langle \text{seq1}, \text{seq2}, \text{TK}, \text{Src} \rangle$ . The following gives the format of GRREQ. According to the modified RREQ message format, a leader constructs the following message and initiates a search within the group. The message also builds a per hop symmetric link key  $K_n$  for data transmission. The RREQ message uses a new sequence number  $\text{seq3}$  for this routing phase. The  $H^{nr}$  (GIDc) is used for RREQ flood control as before. The destination trapdoor  $\text{trdest}$  is signed by the private key of the leader  $\text{SK}_{LD}$ . PAD is a random string for making this phase-3 RREQ message the same length with that of phase-1 RREQ. Thus, by simply eavesdropping, an attacker is not able to distinguish RREQs in different phases, nor is a legitimate node. But being legitimate, an ordinary node will decrypt the last field of a new received RREQ using its leader's public key to check if it is the intended destination. A group leader receiving a RREQ that is not initiated by itself will decrypt the last field using its private key, for the message can be a phase-1 RREQ. In addition, all the nodes participate in the control flooding of RREQ within the group.

## C. Anonymous Route Reply

### 1) Anonymous Route Reply in the destination group:

After the destination successfully verifies the trapdoor, it initiates route reply with a proof  $\text{prdest}$  for the successful opening on the destination trapdoor. Since the destination node does not know in which group the source node resides, not to mention the source node's identity information, the first step of RREP is targeted at the destination's group leader  $LD$ . ANODR's RREP message is modified to carry the necessary information for  $LD$  (so is encrypted by  $LD$ 's public key  $\text{PK}_{LD}$ ) to further forward the reply.

The RREP procedure of ANODR completes the establishing of an anonymous route between the destination and its leader  $LD$ . As in standard ANODR, the symmetric encryption by a randomly chosen symmetric key  $K_{\text{seed}}$  and the public key encryption of  $K_{\text{seed}}$  by  $\text{pkone}$  ensures untraceability. The added information by HANOR does not weaken the protocol. It is a new group specific hash function, and  $nr$  is retrieved from table S-Table.

The result of hashing  $nr$  times with function  $H2$  is used as a symmetric key in the most outer encryption of GRREP. (2) If  $R$  is in a different group,  $\text{KEY} = \text{KEY}_p = \text{PK}_T$  and  $E_{\text{KEY}}$  refers to an asymmetric encryption using public key  $\text{KEY}$ . Here  $\text{PK}_T$  is retrieved from the P-Table. Then the most outer encryption in GRREP is a public-key encryption. Both encryption methods can only be decrypted correctly by the next hop node  $R$ .  $R$  records  $K_n$  as a VCI (virtual circuit identifier) for data transmission.

The advantages of the mechanism are that the relation between the upstream and downstream nodes is not revealed to any nodes, and only a few nodes along group borders need to perform asymmetric cryptographic operations. In order to understand a received GRREP correctly, an intermediate node will first try to decode it using  $\text{KEY}_s$ . If failed, i.e., it cannot match the  $\text{KEY}_s$  from the decrypted text, it tries to decrypt using the private key  $\text{SK}_T$  that matches  $\text{PK}_T$ . If again failed, the node is not on the path and the GRREP is dropped. If one of the decoding is successful, the intermediate node replaces a new  $K_n$ , encrypts the whole message using an appropriate  $\text{KEY}$  according to the aforementioned rules, and broadcasts it locally.

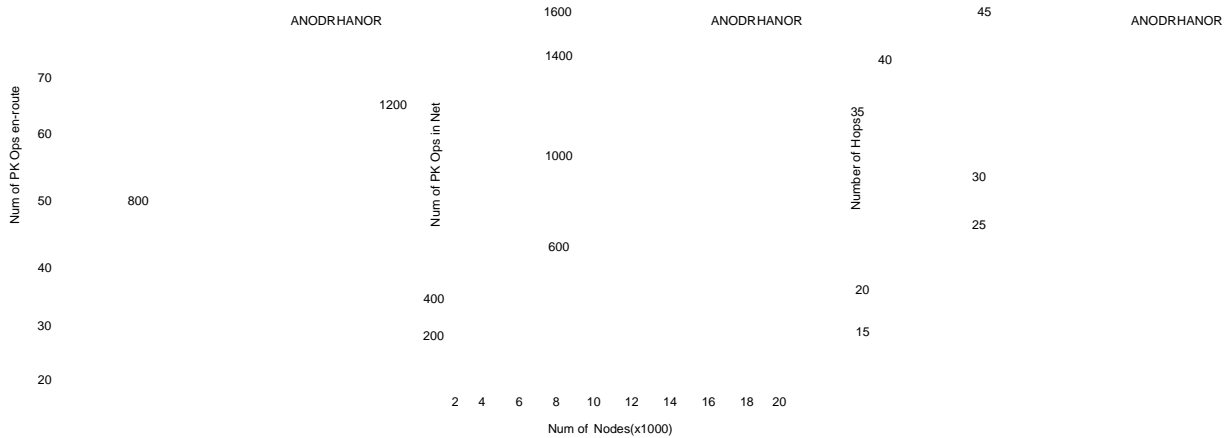
This process repeats until the source group leader receives the GRREP. The route established is anonymous and untraceable with reduced computation overhead.

## IV. SIMULATION RESULTS

We evaluate through simulation the advantage of controlled computational overhead achieved by HANOR. The evaluation metrics include: (i) Number of public key operations en-route: Only public key operations performed by nodes en-route are counted; (ii) Number of public key operations network-wide: public key operations performed by nodes in the entire network, including those performed by nodes not in route but **tried** to decrypt the overheard messages; (iii) Number of path hops: the average number of hops of routes discovered.

# International Journal of Recent Research in Science, Engineering and Technology

Vol. 1, Issue 6, September 2015



path not a shortest-like path like that of ANODR. When the network size increases, the additional hops by HANOR become less significant compared with ANODR. In summary, inter-group routing of HANOR increases the routing efficiency by reducing public key cryptography operations. The performance of HANOR is being further investigated as an on-going work.

## V. CONCLUSION

This paper presents a hierarchical anonymous routing protocol HANOR for mobile ad hoc networks. HANOR uses two levels of anonymous routing: intra-group anonymous routing and inter-group anonymous routing. The main advantage of HANOR is that it effectively controls computational overhead using the hierarchical routing scheme and preserves routing anonymity. Our simulations show a much slower increasing rate of public key cryptography operations compared to a flat scheme. Our future work includes more theoretical analysis on anonymity and routing overhead, extensive evaluation on communication performance and trade-offs under various network conditions.

## REFERENCES

- [1] G. Pei and M. Gerla, "Mobility management for hierarchical wireless networks," *Mob. Netw. Appl.*, vol. 6, no. 4, pp. 331–337, 2001.
- [2] T. Ohta, M. Fujimoto, S. Inoue, and Y. Kakuda, "Hi-tora: a hierarchical routing protocol in ad hoc networks," in p. 143, 7th IEEE International Symposium on High Assurance Systems Engineering (HASE), 2002.
- [3] B. Karp and H. T. Kung, "Gpsr: greedy perimeter stateless routing for wireless networks," in *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*. New York, NY, USA: ACM Press, 2000, pp. 243–254.
- [4] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Scalable ad hoc routing: The case for dynamic addressing," in *proceedings of IEEE INFOCOM, 2004*.
- [5] G. Pei, M. Gerla, and X. Hong, "Lanmar: landmark routing for large scale wireless ad hoc networks with group mobility," in *MobiHoc '00: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. IEEE Press, 2000, pp. 11–18.
- [6] Y. Ge, L. Lamont, and L. Villasenor, "Improving scalability of heterogeneous wireless networks with hierarchical olsr," in *The OLSR Interop & Workshop, 2004*.
- [7] Z. J. Hass, "A new routing protocol for the reconfigurable wireless networks," in *Proceedings, IEEE 6th International Conference on Universal Personal Communications, 1997*, pp. 562–566.
- [8] N. Nikaiein, C. Bonnet, and N. Nikaiein, "Harp - hybrid ad hoc routing protocol," in *proceeding of IST '01: International Symposium on Telecommunications, 2001*.