Study and Performance Comparison of AODV and USOR

Yogesh Raju Patil
M.B.E.S. College of Engineering
Ambajogai

B. M. Patil
M.B.E.S. College of Engineering
Ambajogai

ABSTRACT
Privacy protection is important for some ad hoc networks in order to achieve privacy preserving routing. In this paper we emphasize and do comparison of two schemes Unobservable Secure On-Demand Routing Protocol(USOR) and AODV to provide and preserve privacy in adhoc networks. USOR is an unobservable, secure routing scheme which provides unlinkability and content unobservability for all the different type of packets. For this it uses a combination of group signature and id based encryption. USOR protects user privacy against both inside and outside attackers by defining stronger privacy requirements. After analysis it is found that the USOR results are improved as compared to AODV.

Keywords
Anonymity, Security, Privacy, USOR and AODV.

1. INTRODUCTION
Privacy protection of Mobile Ad-hoc Networks (MANET) is more complex as compared to the wired networks because of the open nature and mobility of the wireless media. The production of users mobility behavior and moment pattern is not required in wired networks, whereas this needs to be done to keep the sensitive information from the adversaries /eavesdroppers in wireless environment. The adversary will be able to harm and compromise the information depending on users behavior if the information is not protected. Also, it is very challenging to provide privacy protection for adhoc networks with low power wireless devices.

With regard to privacy related notions in communication network, we follow the terminology on anonymity, unlinkability and unobservability as discussed in [1]. These notions are defined with regard to item of interest(IOI, including senders, receivers, messages etc) as follows[8].

- *Anonymity* is the state of being not identifiable within a set of subjects , the anonymity set.
- *Unlinkability* of two or more IOI's means these IOI's are no more or no less related from the attackers view**.**
- *Unobsevability* of an IOI is the state that whether it exist or not is indistinguishable to all unrelated subjects .

A large number of anonymous routing schemes for adhoc networks have been introduced over the years providing different levels of privacy protections and with different cost. Most of these proposed schemes rely heavily on public key cryptosystem(PKC) to achieve anonymity and unlinkability in routing. The asymmetric nature of PKC does provide better or good support for privacy protection but it also brings computation overhead along with it. These privacy preserving routing schemes , also called anonymous routing protocols mainly consider anonymity and partial unlinkability , and as said above they exploit the asymmetric feature of PKC to achieve their targets. Current existing schemes/protocols fail to protect all content of packets from the attackers, due to which any attacker can obtain information related to packet type and sequence number. Thus there is no guarantee of complete unlinkability and unobervability because of incomplete content protection.

Only unlinkability is not enough in the demanding environments like battle fields as important information like packet type is available to the attackers. So it is important to make the traffic content completely unobservable to outside attackers. The dependency of all the existing schemes on PKC is also a setback. Among all the requirements, unobservability is the most important as it not only covers anonymity but also unlinkability. In order to achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern . Hence, unobservability can be classified into two types.

- Content unobsevability
- Traffic pattern unobsevability.

Here the focus will be only on content unobsevability. In this paper, we compare an efficient privacy preserving routing protocol USOR that achieves content unobservability by employing anonymous key establishment based on group signature. The set up for USOR is simple , each node only has to obtain a group signature signing key and an id based private key from an offline server or by key management scheme as in [4]. USOR is executed in two phases.

- An anonymous key establishment process is performed to construct secret session keys.
- Then an unobservable route discovery process is executed to find a route to the destination.

The primary aim of this scheme is to protect all parts of the packet contents.

2. RELATED WORK
A number of routing schemes have been introduced for ad hoc networks in recent years, which provide different level of privacy protection at different cost. Most of them depend on public key cryptosystems (PKC) in order to achieve anonymity and unlinkability in routing. PKC can provide better support for privacy protection but it also has significant computation overhead for its operations.

Many of the schemes are PKC-based and the ANODR scheme proposed by Kong et al. [3] is the first one to provide anonymity and unlinkability for routing in ad hoc networks. For route discovery process, ANODR uses one-time public/private key pairs which helps to achieve anonymity and unlinkability based on onion routing, but in its design unobservability of routing messages is not considered. During the route discovery process, each intermediate node has to create a one-time public/private key pair to encrypt/decrypt the routing onion, this helps to break the linkage between incoming packets and corresponding outgoing packets. However, the attacker can easily distinguish different type of

packets as the packets are publically labelled, which does not guarantee unobservability as discussed.

Meanwhile, generation of one-time PKC key pairs (this can be done during idle time) and PKC encryption/decryption both are responsible for computation overhead for mobile nodes in ad hoc networks. ASR [4], ARM [5], AnonDSR [6] and ARMR [7] also make use of one-time public/private key pairs in order to achieve anonymity and unlinkability. ASR is designed to achieve much stronger location privacy than ANODR , it also ensures that nodes on route have no information on their distance to the source/destination node.

As ANODR uses onion routing scheme which exposes distance information to intermediate nodes, ASR does not make use of the onion routing technique while still make use of one-time public/private key pair for privacy protection. ARM [7] considered to reduce computation overhead on one-time public/private key pair generation. Different from the above mentioned schemes, ARMR [9] uses one-time public keys and a bloom filter to establish multiple routes for MANETs. Besides one-time public/private key pairs, SDAR [9] and ODAR [10] also use long-term public/private key pairs at every node for anonymous communication. These schemes are more scalable to network size, but require more computation effort.

3. SECURE ON DEMAND ROUTING PROTOCOL

In this section we introduce an efficient unobservable routing scheme USOR for ad hoc networks. In this protocol, control packets and data packets both look random as well as indistinguishable from dummy packets for adversaries which are outside the network. Only valid nodes can differentiate between routing packets and data packets from dummy traffic with the help of inexpensive symmetric decryption. The awareness behind the proposed method is that if a node can found a key with each of its neighbors, then it can use this key to encrypt the whole packet for the corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is proposed for itself by trial decryption. A group key and a pair wise key are needed to support both broadcast and unicast. As a effect, USOR comprises two phases: unsigned trust establishment and unobservable route discovery.

The aim of unobservable routing scheme USOR to offer the following privacy properties.

1) Anonymity2) Unlinkability3) Unobservability

3.1 Key Generation

In this phase, for unsigned key establishment every individual node in the ad hoc network communicates with its direct neighbors within its radio range. Suppose there is a node S having private signing key gsk_s and a private ID-based.

key K_S in the ad hoc network which is surrounded by a number of neighbors within its radio range.

Following the unsigned key establishment procedure, S does the following [8].

(1) S generates a random number $r_s \in Z_q^*$ and computes $r_s P$. It then computes a signature of $r_s P$ using its private signing key gsk_s to obtain $SIG_{gsks}(r_S P)$. Anyone can verify this signature with the help of a group public key gpk. It broadcasts $r_s P, SIG_{gsks}(r_S P)$ within its neighborhood.

(2) A neighbor X of S receives the message from S and verifies the signature in that message. If the verification is successful, X chooses a random number $r_X \in Z_q^*$ and computes $r_X P$. X also computes a signature $SIG_{gsk_X}(r_s P \mid r_X P)$ using its own signing key gsk_X. X computes the session key $k_{SX} = H_2(r_s r_X P)$, and replies to S with message $r_X P, SIG_{gsk_X}(r_s P \mid r_X P)$, $E_{k_{SX}}(\bar{k}_{X*} \mid r_s P \mid r_X P)$, where $\bar{k}_{X*}$ is X's local broadcast key.

(3) After receiving the reply from X, S verifies the signature inside the message. If the signature is correct, S proceeds to compute the session key between X and itself as $k_{SX} = H_2(r_s r_X P)$. Also S generates a local broadcast key $\bar{k}_{S*}$, and sends $E_{k_{SX}}(\bar{k}_{X*} \mid r_s P \mid r_X P)$ to its neighbor X to inform X about the established local broadcast key.

(4) X receives the message from S and computes the same session key as $k_{SX} = H_2(r_s r_X P)$ and it then decrypts the message to get the local broadcast key $\bar{k}_{S*}$.

Note that the messages exchanged in this phase are observable, but this does not leak any private information such as node identities. As a result of this phase, a pair wise session key k_{SX} is constructed unsigned, which means the two nodes establish this key without knowing the identity of the other party. At the same time, node S establishes a local broadcast key $\bar{k}_{S*}$, and transmits it to all its neighbors. It is used for per-hop protection for subsequent route discovery.

3.2 Routing Scheme

In this phase, privacy-preserving route discovery is done based on the keys established in previous phase. Similar as in case of normal route discovery, this process also comprises of route request and route reply. The route request messages are flooded throughout the whole network, while the route reply messages are sent back to the source node only. Suppose there is a node S (source) trying to find a route to a node D (destination), and S already knows the identity of the destination node D. We assume that there are three intermediate nodes between S and D, The route discovery process executes as follows[8].

Route Request (RREQ): Source node S chooses a random number r_s, and uses the identity of destination node D to encrypt the information that only can be opened with D's private ID-based key. S then has to select a sequence number seqno for this route request, and also a random number N_S as the route pseudonym, which acts as the index to a specific route entry. Each node has to maintain a temporary entry in its routing table (seqno, Prev RNym, Next RNym, Prev hop, Next hop), where seqno specifies route request sequence number, Prev RNym indicates the route pseudonym of previous hop, Next RNym indicates route pseudonym of next hop, Prev hop specifies upstream node and Next hop is the downstream node along the route.

When the route request message is received from source node S, A uses all his session keys shared with all neighbors. After finding out this is a route request packet, A tries to decrypt the packet using his private ID-based key to check whether he is

the destination node. To avoid RREQ broadcasting storm, A checks whether he has received the same request before by looking up in his cache, which has a list of N_S and sequence number. If it is not a duplicate RREQ, A caches N_S and sequence number for a given time to detect multiple receipt of the same RREQ packet. In this example, A is not the destination node and the trial fails, so he acts as an intermediate node. Other intermediate nodes perform similar operation same as A does. Finally, the destination node D receives the message from C.

Route Reply (RREP)*:* After node D finds out that he is the destination node, he starts the preparation to send a reply message to the source node. To save communication cost for route reply messages, unicast is used instead of broadcast. Destination node D uses a random number r_D and computes a ciphertext showing that he is the valid destination capable of opening the information. For data protection a session key is computed. When C receives the above message from D, he identifies who the sender of the message and sends the message to B. similarly, every intermediate nodes perform the same operations as C does. Finally, route reply is sent back to the source node S by A. S decrypts the ciphertext and is composed faultlessly. Now S is ensured that D has successfully opened the route request packet, and the route reply is originated from the destination node D.

4. RESULT

Figure 1 represents throughput achieved for USOR and AODV, it appears similar for both the protocols. Figure 2 represents jitter which shows variations with respect to average node speed which is better for USOR as compared to AODV. Figure 3 represents packet delivery ratio which is linear for USOR than AODV.

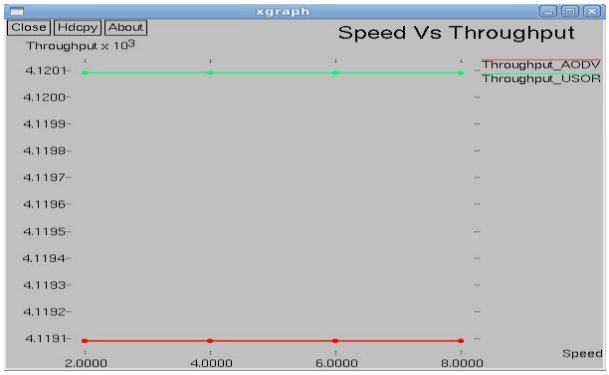

Fig 1: Throughput

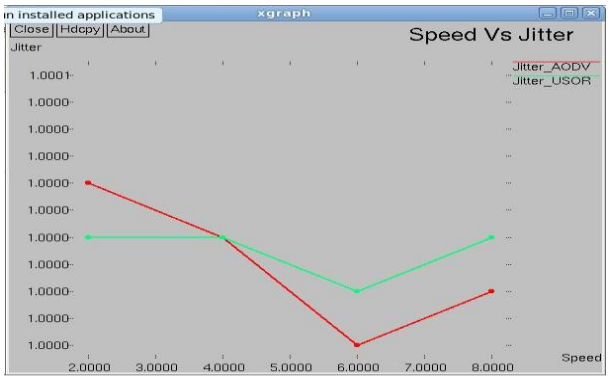

Fig 2: Jitter

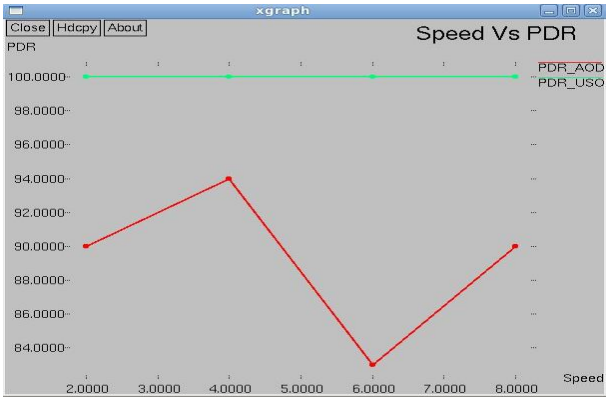

Fig 3: Packet Delivery Ratio

5. CONCLUSION AND FUTURE WORK

The comparison between AODV with USOR shows us that USOR delivers strong privacy protection along with content unobsevability than AODV for adhoc networks.Future work is to check the ability of USOR to handle DOS attacks.

6. REFERENCES

[1] A.Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.

[2] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.

[3] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.

[4] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli, "Anonymous secure routing in mobile ad-hoc networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[5] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.

[6] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33– 42.

[7] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.

[8] Zhiguo Wan, Kui Ren, and Ming Gu," USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE transactions on wireless communications, vol. 11, no. 5, may 2012

[9] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in Proc. 2004 IEEE LCN, pp. 618–624.

[10] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems