International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

PRIVACY PROTECTION THROUGH UNOBSERVABLE SECURE ON-DEMAND ROUTING PROTOCOL FOR MANET

A.Arulmozhi (PG Scholar)
Dr.Pauls Engineering College

Narasimmalou
Dr .Pauls Engineering College

Abstract- Secure Routing is a challenging task for ad hoc wireless network due to open nature and mobility of wireless media. In this paper, we propose an Enhanced Unobservable Routing scheme to offer privacy preservation to all types of packets. Enhanced USORworks to protect against wormhole attack. In ad hoc network, when a source searches for a route to a destination using USOR protocol, an intermediate node can reply with its cached entry.After receiving both route reply and confirmation message, the source determines the validity of path according to its policy. Simulation result shows that USOR has satisfactory performance compared to AODV in terms of throughput, bandwidth and Delay.

1. INTRODUCTION

Privacy protection in routing of MANET has interested a lot of research efforts. A number of privacy-preserving routing schemes have been brought forward. However, existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET, most of them exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlinkabilityand unobservability are not guaranteed due to incomplete content protection. Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which breaksunlinkability and may lead to source traceback attacks.Meanwhile, unprotected packet type and sequence number also make existing schemes observable to the adversary. Until now, there is no solution being able to achieve complete unlinkability and unobserv-ability.

Privacy preserving routing properties:

Anonymity: Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. The senders, receivers, and intermediate nodes are not identifiable within the whole network.

Unlinkability: The linkage between any two or more item of interest from the senders, the receivers, the intermediate nodes, and the messages is protectedfrom outsiders. Note linkages between any two messages, e.g., whether they are from the same source node, are also protected.

Unobservability: Any meaningful packet in the routing scheme is indis-tinguishable from other packets to an outside attacker. Not only is the content of the packet but also the packet header like packet type protected from eavesdroppers. And any node involved in route discovery or packet forwarding, including the source node, destination node, and any intermediate node, is not aware of the identity of other involved.

An ad-hoc routing protocol is a convention or standard, that controls the way of routing packets between computing devices in a mobile ad hoc network .In ad-hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbours. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them.

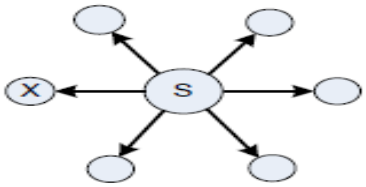
2. USOR MODEL

In this section we present an efficient unobservable routing scheme USOR for ad hoc networks. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbours, then it can use such a key to encrypt the whole packet for a corresponding neighbour. The receiving neighbour can distinguish whether the encrypted packet is intended for itself by trial decryption.

In order to support both broadcast and unicast, a group key and a pairwise key are needed. As a result, USOR comprises two phases: anonymous trust establishment and unobservable route discovery.

USOR uses Elliptic curve Diffie–Hellman (ECDH) key exchange for anonymous key establishment. It is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric key cipher. It is a variant of the Diffie–Hellman protocol using elliptic curve cryptography.

A)Anonymous key establishment: Each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbours. Every node communicate with its direct neighbours within its radio transmission range. Every node has a private group signature key gsk and a private ID-based key k.



S broadcast the first message to its direct neighbours

$<r_sP, SIG_{gsk_s}(r_sp)>$

r_s- random number E Z^*_q

P-generature of G1

$SIG_{gsk_s}(r_sp)$-Signature of $r_s$using S's private signing key

gsk_s

A neighbor *X* of *S* receives the message from *S*and verifies the signature with gpk Then *X* replies to *S* with the message,**$<r_xP, SIG_{gsk_x}(r_sP|r_xP), E_{ksx}(k_x^*|r_sP|r_xP)>$**

k_{sx}(session key)=$H_2(r_sr_xP)$

H2- maps anlement in g1 to a session key.

kx*-X's local broadcast key

S computes the session key between X and itself and sends to X

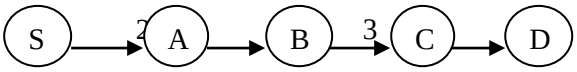
$<E_{ksx}(k_s^*|k_x^*|r_sP|r_xP)>$

X decrypts to get the local broadcast key k_s^*

B)Route discovery: Based on the key establishment phase the route discovery

process is initiated.The route discovery process comprises of route request and route reply messages

Route request,



S-Source, D-Destination, A,B,C-Intermediate nodes

(1)$Nonce_S$,Nym_S,E_{kS}*(RREQ,N_S,E_D(S,D,r_SP),seqno)

$Nym_s = H_3(k_s*| Nonce_s)$

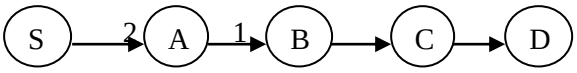
H_3-maps a session key and random nonce to random pseudonym

N_s-route pseudonym

(2)$Nonce_A$,Nym_A,E_{kA}*(RREQ,N_A,E_D(S,D,r_AP),seqno)

(3)$Nonce_B$,Nym_B,E_{kB}*(RREQ,N_B,E_D(S,D,r_BP),seqno)

Route reply,



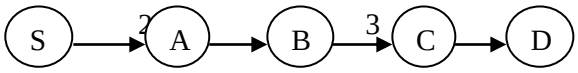
Node D prepare a reply message and follows unicast method to deliver the message to the source node

(1)$Nonce_D$,Nym_{CD},E_{KCD}*(RREP,N_C,E_S(D,S,r_SP,r_DP),seqno)

(2)$Nonce_C$,Nym_{BC},E_{KBC}*(RREP,N_B,E_S(D,S,r_SP,r_DP),seqno)

(3)$Nonce_A$,Nym_{SA},E_{KSA}*(RREP,N_S,E_S(D,S,r_SP,r_DP),seqno)

Data transmission,



S starts unobservable data transmission on under the protection of pseudonyms and keys.S must traverse A,B and C to reach D

(1) $Nonce_S$,Nym_{SA},E_{KSA}*(DATA,N_S,seq no, E_{KSD}(payload))

(2) $Nonce_A$,Nym_{AB},E_{KAB}*(DATA,N_A, seqno,E_{KSD}(payload)

(3) $Nonce_A$,Nym_{SA}, E_{KCD}*(DATA,N_C, seqno,E_{KSD}(payload))

Depending upon the position of mobile nodes topology can be created.After the formation of topology route discovery process is initiated by USOR. Route discovery process comprises of signature verification, RREQ, RREP and privacy preservation. Finally the node starts to transmit the data packets through unobservable secured path.

Drawback:

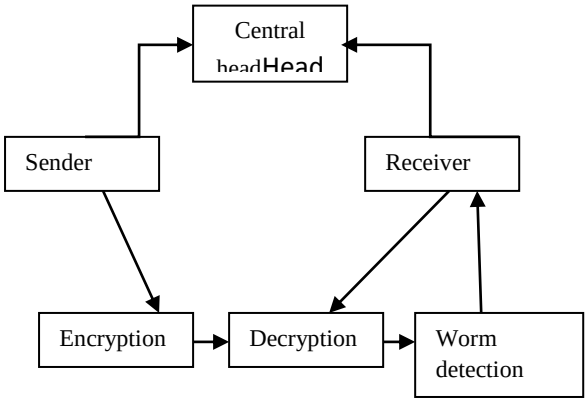
The USOR protocol doesn't prevent from wormhole attack. Incomputer networking, a packet drop attack or wormhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a loss network, the packet drop attack is very hard to detect and prevent.

The packet drop attack can be frequently deployed to attack wireless ad-hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has

been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network. To prevent from black hole attack all the packets are broadcasted instead of unicast method.

3. ENHANCED USOR MODEL

The setup of USOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management. The unobservable routing protocol is then executed in two phases. First, 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. High level security.



3.1.Block Diagram of Enhanced USOR

Sender and receiver nodes consist of two properties, they are public and private key properties. Using private keys(password) accessed public keys(publically known) contains received information. Sender node initiates the process by sending their profile information to the receiver. After receiving the request from sender node, receiver node checks whether the profile information is right or wrong. After receiving the correct information from the sender node the receiver node acknowledges the particular sender to send data. Group signature is a method used for encryption between sender and receiver node. The sender notifies the receiver the data's is acknowledged by receiver.

3.1 Routing schemes

USOR is efficient as it uses a novel combination of group signature and ID-based encryption (IDE) for route discovery. Security analysis demonstrates that USOR can well protect user privacy against both inside and outside attackers.

Group Signature Scheme

A Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group. Essential to a group signature scheme is a group manager, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. In some systems the responsibilities of adding members and revoking signature anonymity are separated and given to a membership manager and revocation manager respectively.

Identity-Based Encryption

Identity-Based Encryption allows for a party to encrypt a message using the recipient’s identity as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. This can be very useful in applications such as email where the recipient is often off-line and unable to present a public-key certificate while the sender encrypts a message.

We present the first efficient Identity-Based Encryption scheme that is fully secure without random oracles. The proof of our scheme makes use of an algebraic method first used by BonehandBoyenand the security of our scheme reduces to the decisional Bilinear

Diffie-Hellman(BDH)assumption. We additionally show that our IBE scheme implies a secure signature scheme under the computational Diffie-Hellman assumption without random oracles. Previous practical signature schemesthat were secure in the standard model relied on the Strong-RSA assumption or the Strong-BDH assumption.

ID-based encryption (IBE) is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user. This can use the text-value of the name or domain name as a key or the physical IP address it translates to.

Benefits of Enhanced USOR: Our protocol Enhanced USOR does not encourages malicious nodes which can advertise false paths to slow down path finding procedures or intrude all data packets. For instance, if a node in a network turns to malicious node and tries to advertise a path, this attempt can be nullified as CREP from next node will carry different routing information. Hence our protocol has overcome a wormhole attack.In this wormhole attack some malicious node advertises wrong route information and hence forth diverts packet transmission or drops packets. More ever, Enhanced USOR increases robustness of route information.

4. SIMULATION RESULTS

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every n packets or every t seconds, or a randomly selected portion of the packets. This is rather called a wormhole attack.

In a wormhole attack, attackers tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbours and making them communicate through the wormhole link.

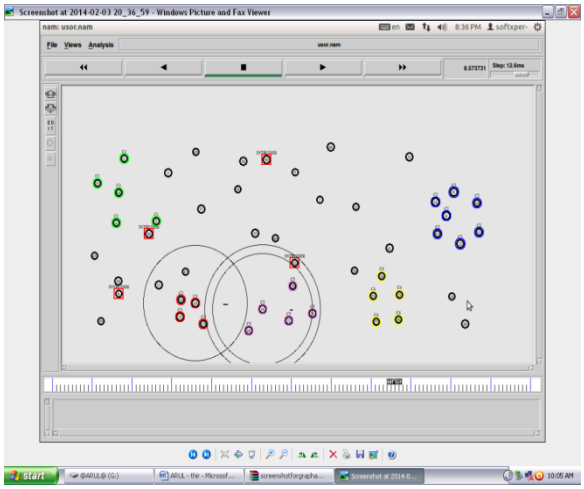


Figure.4.1 Prevention from wormholeattack by Enhanced USOR

. Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and this is the reason the attacks are serious. To prevent from wormhole attack all the packets are broadcasted instead of unicast method. Prevention of wormhole attack is shown in Figure.4.1.

Simulation parameters:

Parameter	**Specification**
Groupsignature generation	22ms
Groupsignature verification	24ms
Routing Protocol	USOR
Wireless Radio Range	50m
Wireless Bandwidth	2Mbps
Number of Mobile Nodes	26 nodes
Scenario Dimension	881mx652m
Simulation Time	500s

5. PERFORMANCE EVALUATION

Performance of AODV and USOR are calculated in terms of Throughput, Bandwidth and delay.

Bandwidth:

The performance of AODV and USOR is analyzed. Bandwidth is measured against the number of packets. Bandwidth comparison of USOR and AODV is shown in Figure.5.1

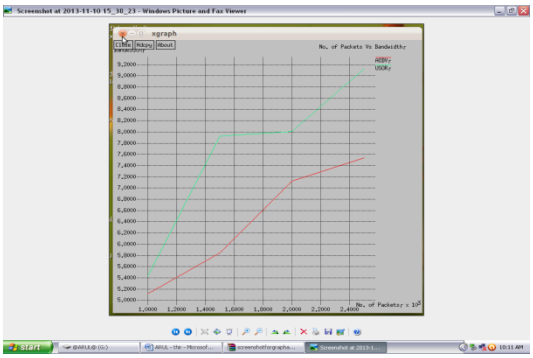


Figure.5.1.Bandwidth comparison

But in a wireless network, the radio band is limited, and hence the data rates it can offer are much less than what a wired network can offer. This requires that the routing protocols use the bandwidth optimally by keeping the overhead as low as possible. The limited bandwidth availability also imposes a constraint on routing protocols in maintaining the topological information. Due to the frequent changes in topology, maintaining consistent topological information at all nodes involves more control overhead which, in turn, results in more bandwidth wastage.The performance of AODV and USOR is analyzed. Packet delivery ratio is measured against the Throughput.

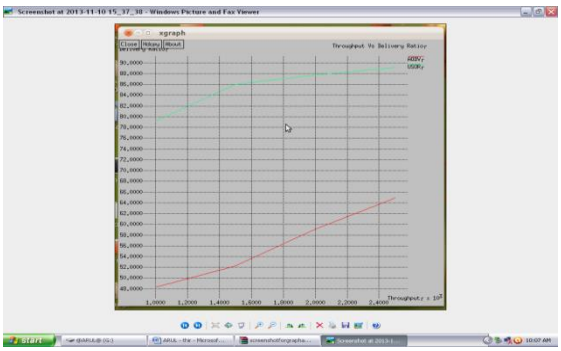


Figure.5.2 comparison of Throughput in USOR and AODV

Delay:

Network delay is an important design and performance characteristic of a computer or telecommunications network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. Delay between USOR and AODV is shown below.Packet delivery delay is measured against mobility.

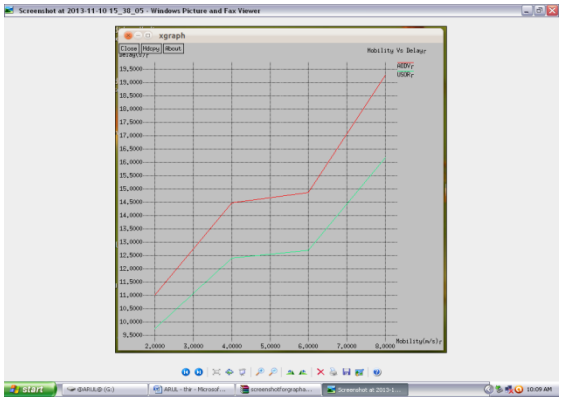


Figure.5.3 Delay Comparison between USOR and AODV

6.CONCLUSION

An unobservable routing protocol USOR offers strong privacy protection by providing complete unlinkability and content unobservability for ad hoc networks. To prevent from wormhole attack, the route discovery process of USOR protocol is strengthened by the method called Enhanced Unobservable Routing scheme. The security analysis demonstrates that Enhanced USOR protocol is resistant against both inside and outside attackers. This protocol is implemented on NS-2 and the performance of USOR AODV protocol examined in terms of throughput, bandwidth and delay. The result shows that USOR has satisfactory performance compared to AODV.

REFERENCES

[1] Zhiguo Wan, KuiRen, and Ming Gu "An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.,VOL.11,NO.5,MAY 2012.

[2] J.Sel. "Privacy-preserving location-based on-demand routing in MANETs," IEEE trans. Areas Commun., vol. 29, no. 10,pp. 1926–1934, 2011.

[3] J. Han and Y. Liu, "Mutual anonymity for mobile peer-to-peer systems,"IEEE Trans. Parallel Distrib.Syst., vol. 19, no. 8, pp. 1009–1019, Aug.2010.

[4] Y. Dong, T. W. Chim, V. O. K. Li, S.-M.Yiu, and C. K. Hui, "ARMR:anonymous routing protocol with multiple routes for communicationsin mobile ad hoc networks," Ad Hoc Networks, vol.7,no.8,pp.1536–1550,2010.

[5] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymousdynamic source routing for mobile ad-hoc networks," in Proc. 2009 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.

[6] A. Boukerche, K. El-Khatib, L. Xu,andL.Korba, "SDAR: a securedistributedanonymous routing protocol for wireless and mobile ad hocnetworks," in Proc. 2009 IEEE LCN, pp. 618–624.

[7] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routingin ad hoc networks," in 2009 IEEE Conference on Mobile Ad-hoc and Sensor Systems.

[8] S. Capkun, L. Buttyan, and J. Hubaux, "Self- Organized Public-Key Management for Mobile Ad-hoc Networks," IEEE Transaction Mobile Computing, vol. 2, no. 1,2003, pp. 52-64.

[9] Y. Zhang, W. Liu, and W. Lou, "Anonymous Communications in Mobile Ad-hoc Networks," in IEEE INFOCOM, 2005, pp. 125-138.

T. Narasimmalouwasbornin Pondicherry, India in 1976. He received his Bachelor of Technology in Electronics and Communications Engineering, and Master of Technology degree in Electronics and Communications Engineering from Pondicherry University, Pondicherry, India. Currently he is working as Professor in Dr. Pauls Engineering College, Villupuram and affiliated to Anna University Chennai, Tamil Nadu, India. He is a life member of Indian Society for Technical Education, His area of interest includes Wireless Communications and Network Security.

A.Arulmozhi was received her Bachelor of Engineering in Electronics and Communications Engineering, from Anna University, Chennai and Currently she is persuing her Master of Engineering degree in Applied Electronics, Dr. Pauls Engineering College, Villupuram and affiliated to Anna University Chennai, Tamil Nadu, India. Her area of interest includes Wireless Communications and EmbeddedSystems.