Detecting Attacks in USOR Routing Protocol for MANET

Saveetha Paramasivam
M.Tech Scholar, CSE dept, SIRT
Bhopal, M.P, India

Prof. Yogadhar Pandey
Assistant Professor, CSE dept, SIRT
Bhopal, M.P, India

Abstract

A number of privacy-preserving routing schemes have been proposed. But the existing anonymous routing protocols mainly consider anonymity and partial unlinkability in MANET due to incomplete content protection. However USOR (Unobservable Secure On-Demand Routing Protocol) provides complete unlinkability and content unobservability. But USOR doesn't defend against the attacks. In this paper we propose a modified USOR which provides anonymity, unlinkability and complete unobservability and also resist against attacks like wormhole and black hole. We implement modified USOR on ns2 and evaluate its performance by comparing with AODV and USOR. The simulation results shows that the modified USOR has satisfactory performance compared to USOR and also achieves stronger privacy protection than existing schemes.

1. Introduction

1.1. Attacks in MANET

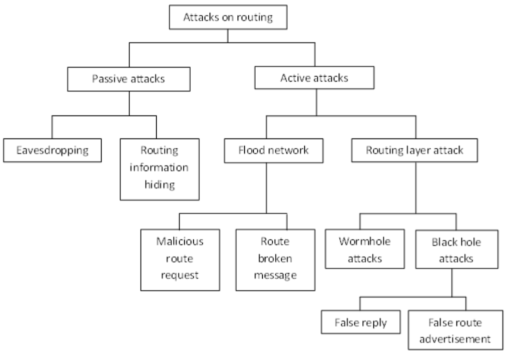


Figure 1. Attacks on Routing Layer

Due to vast number of unstructured nodes and absence of a priori knowledge about the neighbors in the open environment attacks occur. These attacks can be classified based on their communication layers. The classification of attacks in routing layer is shown in Figure1

Possible attacks in each layer are as follows: Application layer attacks are malicious code and repudiation. Transport layer attacks are session hijacking and flooding. Network layer attacks are Sybil attack, flooding, black hole, grey hole, worm hole, link spoofing, link withholding, location disclosure, etc... Data Link layer attacks are malicious behavior, selfish behavior, active attack, passive attack. Physical layer attacks are interference, traffic jamming, eavesdropping.

1.2. Privacy Preserving Properties

Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. Unlinkability of two or more item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether the IOI's are related or not. Unobservability of IOI from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

2. USOR Protocol

2.1. Modules

The process has been divided into three modules. They are as follows:

- Key Generation
  - ❖ Group Signature Scheme.
  - ❖ ID-based Encryption Scheme.
- Anonymous Trust Establishment
- Privacy-Preserving Route Discovery
  - ❖ Route Request.
  - ❖ Route Reply.
  - ❖ Attack Analysis.
  - ❖ Data Transmission.

2.2. Overall Process

Figure.2 represents the Overall Process of USOR Protocol.

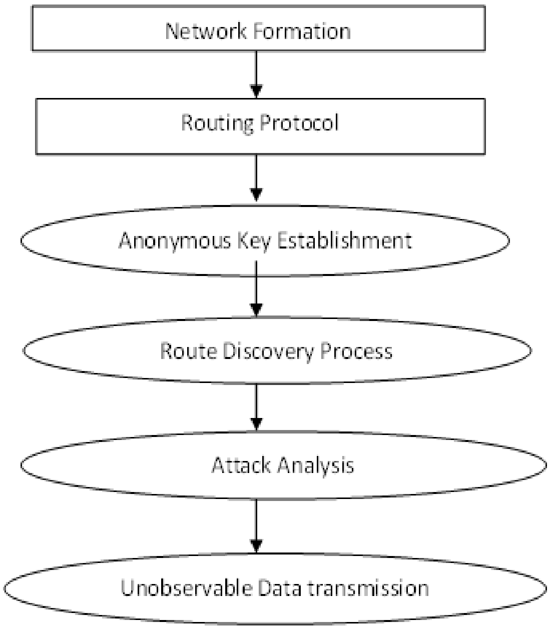


Figure 2. Overall process

2.3. Key Generation

Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group. Key server generates a group public key PU_{gp} which is publicly known by everyone. It generates a private group signature key PR_x for each node X. ID-based encryption 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, which allowed users to verify digital signatures using only public information such as the user's identifier.

2.4. Anonymous Trust Establishment

Figure3 describes about the flow chart of anonymous trust establishment. Every node in the ad hoc network communicates with its direct neighbors within its radio range for communication. Source node 'S' with a private signing key PR_S and a private ID-based key K_S in the ad hoc network communicate with its direct neighbors.

S generates a random number r_S using random generator. It computes a signature of r_S using its private signing key PR_S to obtain $SIG_{PRs}(r_S)$. Anyone can verify this signature using the group public key PU_{gp}. S broadcast $(r_{S,}SIG_{PRs}(r_S))$ within its neighborhood. X neighborhood of S receives $(r_S, SIG_{PRs}(r_S))$, verifies the signature on successful verification it computes $SIG_{PRx}(r_S|r_P)$ using its private signing key PR_X and r_X X's random number. X computes the session key $k_{SX} = H(r_Sr_X)$, and replies to S with message $(r_X, SIG_{PRx}(r_S|r_P), E_{Ksx}(k_x|r_S|r_X))$ where k_x is X's local

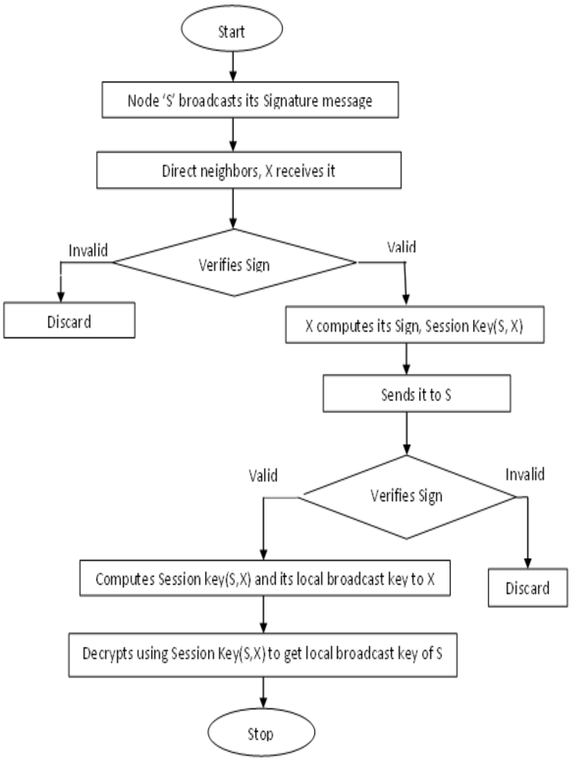

Start
Node 'S' broadcasts its Signature message
Direct neighbors, X receives it
Invalid
Verifies Sign
Valid
Discard
X computes its Sign, Session Key(S, X)
Sends it to S
Valid
Verifies Sign
Invalid
Computes Session key(S,X) and its local broadcast key to X
Discard
Decrypts using Session Key(S,X) to get local broadcast key of S
Stop

Figure 3 Flow Chart for Anonymous Key Establishment

broadcast key.S verifies the signature inside the message from X. On valid signature 'S' proceeds to compute the session key with X as $k_{SX} = H(r_Sr_X)$. S generates local broadcast key ks, and sends $E_{Ksx}(k_S|k_X|r_S|r_X)$ to its neighbor X to inform X about the established local broadcast key. X receives the message from S and computes the same session key as $k_{SX}=H(r_Sr_X)$. It then decrypts the message to get the local broadcast key k_S.

2.5. Route Request

The route request messages flood throughout the whole network, while the route reply messages are sent backward to the source node only. S chooses a random number r_S, and uses the identity of node D to encrypt a trapdoor information that only can be opened with D's private ID based key, which yields $E_D(S,D, r_S)$. S selects a sequence number for this route request, and another random number N_S as the route pseudonym, which is used as the index to a specific route entry. To achieve unobservability, S chooses a nonce $Nonce_S$ and calculates a pseudonym as $Nym_S = k_{SX}(k_S|Nonce_S)$.

Each node maintains a temporary entry in his routing table (seqno, Prev RNym, Next RNym, Prev hop,Next hop) where seqno is the route request sequence number, Prev RNym denotes the route pseudonym of previous hop, Next RNym is the route pseudonym of next hop, Prev hop is the upstream node and Next hop is the downstream node along the route.

S broadcasts the message: {Nonce$_S$, Nym$_S$, E$_{Ks}$ (RREQ, N$_S$, E$_D$ (S, D, r$_S$), seq. no.)}The size of a packet is 128 bytes. Source ID, and destination ID requires 4 bytes each. Source location (x,y), source speed (x,y),and time stamp requires 8 bytes each. Number once used, route nym and encrypted packet requires 32 bytes each. E$_D$ (S, D, r$_S$) is the data encrypted by destination's key.

Each intermediate node decrypts the packet using the session key generated, determines that it is a route request and forwards the packet to the destination.After route request reaches the destination node D, it starts to prepare a reply message to the source node. Route reply messages are unicast instead of broadcast is used to save communication cost. D chooses a random number r$_D$ and computes a ciphertext E$_S$(D, S, r$_S$, r$_D$) showing that it is the valid destination capable of opening the trapdoor information. A session key k$_{SD}$ = H(r$_S$r$_D$|S|D) is computed for data protection. Then it generates a new pairwise pseudonym Nym$_{XD}$ = H(k$_{XD}$|Nonce$_D$) between X and itself. At the end, using the pairwise session key k$_{XD}$, it computes and sends the following message to intermediate node X: {Nonce$_D$, Nym$_{XD}$,E$_{KXD}$(RREP,N$_X$,E$_S$(D, S, r$_S$, r$_D$), seqno)}. Other intermediate nodes perform the same operations as D does. Finally, the following route reply is sent back to the source node S by intermediate nodes say 'X' S decrypts the ciphertext using the right key k$_{SX}$ and verifies that E$_S$(D, S, r$_S$, r$_D$) is composed faultlessly. Now S is ensured that D has successfully opened the route request packet, and the route reply is really originated from the destination node D.

2.6. Route Reply

X unicasts the message:
{Nonce$_D$,Nym$_{XD}$,EK$_{XD}$(RREP, N$_X$, E$_D$(S, D, r$_S$, r$_D$),seq. no.)}The size of a packet is 128 bytes. It is same as route request packet format.

Each intermediate node decrypts the packet using the session key generated, determines that it is a route reply and forwards the packet to the source.

2.7. Data Transfer

Source node S after successfully finding of a route to the destination node D, S starts unobservable data transmission under the protection of pseudonyms and keys. Data packets from S must traverse X to reach D.

Format of data packets sent by S:**Nonce$_S$, Nym$_{SX}$, E$_{kSX}$ (DATA,N$_S$, seqno, E$_{kSD}$(payload))**

X receives message from S. X knows that this message is for him according to the pseudonym Nym$_{SX}$. After decryption using the right key, X knows this message is a data packet and should be forward it to D according to route pseudonym N$_S$.

X computes and forwards the data packet. Format of data packets sent by X:**Nonce$_X$, Nym$_{XD}$, E$_{kXD}$ (DATA,N$_X$, seqno, E$_{kSD}$(payload))**

The data packet is further forwarded by other intermediate nodes until it reaches the destination node D. At the end, the data packet is received by D. By looking up in the route table, D knows himself as the destination of the packet. So he is able to decrypt the encrypted payload with the session key k$_{SD}$.

3. Attack Analysis

3.1. 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 neighbors and making them communicate through the wormhole link. For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the wormhole link. The wormhole link can be established by a variety of means either by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

In Figure4 nodes X and Y are the wormhole attackers and a wormhole link is shown.Wormhole attack is a relay-based attack and a severe attack on MANET routing that can disrupt the routing protocol and therefore disrupt or breakdown a network and this is the reason the attacks are serious. Activities of wormhole are they record the wireless data they overhear. They forward it to each other. It replays the packets at the other end of the network. It replays valid network messages at improper places. It makes far apart nodes believe that they are immediate the neighbors.

An approach to detect the wormhole attack is based on the packet leashes. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Leashes are designed to protect against wormholes over a single wireless transmission. When packets are sent over multiple hops, each transmission requires the use of a new leash. Leashes can be classified as geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash establishes an upper bound on a packet's lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet travelled further than the leash allows.

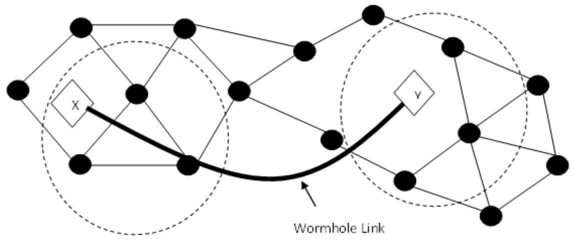


Figure 4. Wormhole attack

3.2. Black hole attack:

Black hole attack can also be said as packet dropping attack. It is a type of denial-of-service attack. In this type of attack, malicious node falsely advertises good path to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node. Fake route request packets are used to catch the malicious nodes. The fake route request used to find the black hole nodes in the network route request packet format is same as the existing, except that a fake destination address is used, which really doesn't exists.

In Figure 5, S is the source node, D is the destination node and M is the malicious node. Route request, route reply and dropped packets are represented.

A Black hole attack is an attack where all the packets in the network are redirected to a specific node the black hole node. When the packets reach this malicious node, they merely disappear into a black hole in universe. To carry out a black hole attack, the black hole node takes advantage of the ad hoc routing protocol, such as AODV or DSR, to advertise itself as having a valid route to the destination node, even though the route is spurious, with the intention to intercept packets. Or malicious node waits for neighboring nodes to send route request messages.

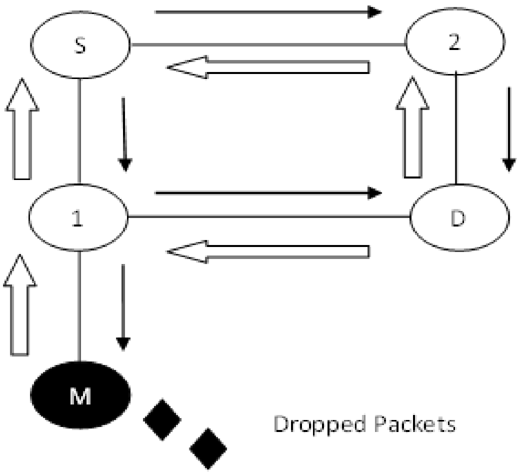


Figure 5. Black hole attack

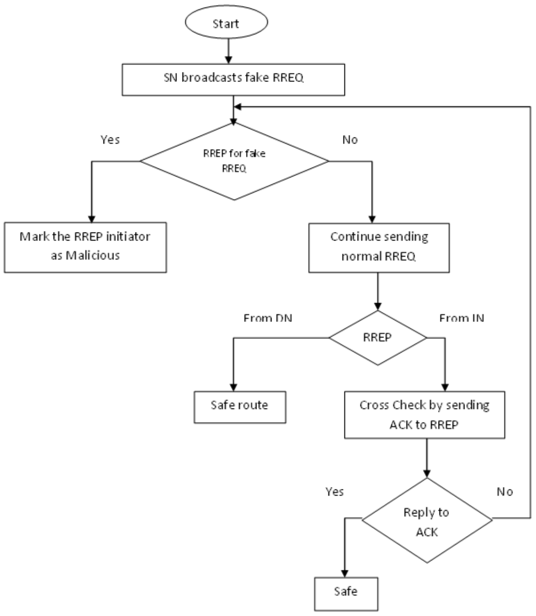


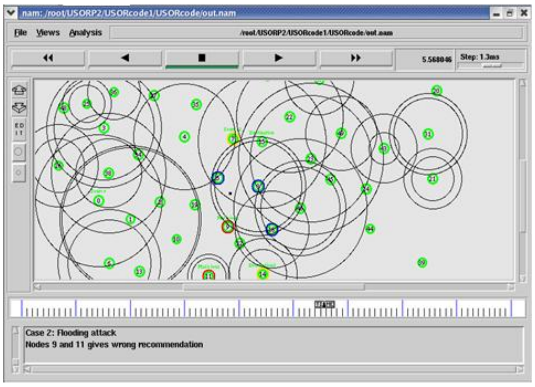
Figure 6. Flow Chart for detecting Black hole attack

When the malicious node receives a route request message, without checking its routing table, immediately sends a false route reply message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other route reply messages and begin to send packets over malicious node. Malicious node attacks all route request messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. Figure6 describes the flow chart for detecting black hole attack. Source node sends a fake route request and the particular node that is responding for such a fake request is the black hole node.

4. Experimental Results and Analysis

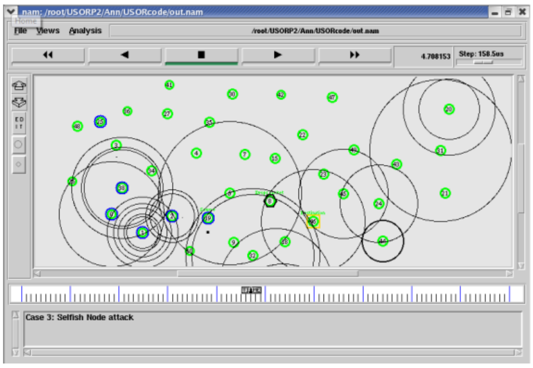
The capability of the proposed attack free unobservable routing protocol is demonstrated via series of simulation experiments using NS-2 Simulator. The number of nodes being used is 50. The nodes are arranged randomly. Each node represents the individual routers. The time taken for overall experiment is 10 ms.

Figure 7 describes the flooding attack Figure8 describes the selfish node attack and in Figure 9 detecting black hole attack is described.


nam: /root/USORP2/USORcode1/USORcode/out.nam
File
Views
Analysis
/root/USORP2/USORcode1/USORcode/out.nam
5.568046
Step: 1.3ms

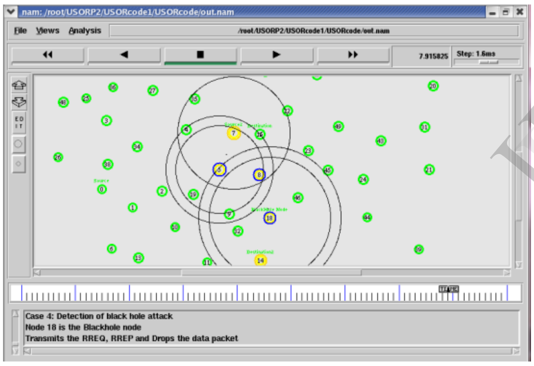
Case 2: Flooding attack
Nodes 9 and 11 gives wrong recommendation

Figure 7 Flooding attack


nam: /root/USORP2/Ann/USORcode/out.nam
File
Views
Analysis
/root/USORP2/Ann/USORcode/out.nam
4.780153
Step: 158.5us

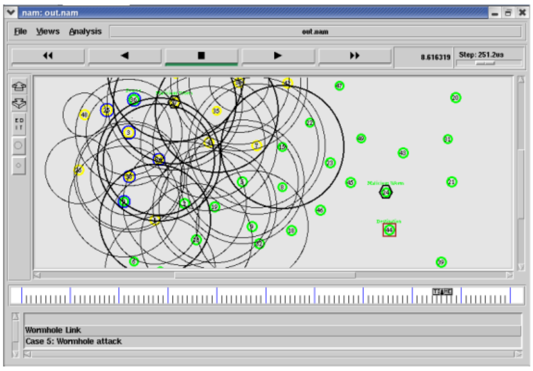
Case 3: Selfish Node attack

Figure 8 Selfish node attack


nam: /root/USORP2/USORcode1/USORcode/out.nam
File
Views
Analysis
/root/USORP2/USORcode1/USORcode/out.nam
7.915825
Step: 1.6ms

Case 4: Detection of black hole attack
Node 18 is the Blackhole node
Transmits the RREQ, RREP and Drops the data packet

Figure 9 Black hole attack



Wormhole Link
Case 5: Wormhole attack

Figure 10 Wormhole attack

5. Comparative Analysis

Table 1 Comparative Analysis

Protocol	**Unlinkability**	**Unobservability**	**Attacks detected**
Modified USOR	Provides unlinkability	Provides content and traffic pattern unobservability	Wormhole attack and black hole attack
USOR	Provides unlinkability	Provides content and traffic pattern unobservability	Malicious node attacks
ANODR	Does not provide unlinkability	Does not provide unobservability	Does not deal with attacks
Anon DSR	Does not provide unlinkability	Does not provide unobservability	Does not deal with attacks

Table 1 describes the comparative analysis of routing protocol.

6. Performance Analysis

USOR is implemented using Network Simulator (NS2) tool in the following environment conditions.

Table 2 Simulation Parameters Table

Sr.No.	**PARAMETERS**	**VALUE**
1	Routing Protocol	Modified USOR
2	Simulation time	10 ms
3	Simulation area	1000 x 1000 m
4	Number of nodes	50
5	Traffic type	CBR
6	Maximum connections	10
7	Wireless-Radio-Range	250m
8	Average-Node-Speed	0-5 m/s
9	Source-Destination-Pairs	25
10	Traffic-Type	512-byte
11	Traffic-Frequency	4
12	Wireless-Bandwidth	2Mbps
13	Node-Pause-Time	0s

14	Key-Update-Interval	40s
15	Average-Hops	2.90
16	Average-Neighbours	12.69

6.1. Packet Delivery Ratio

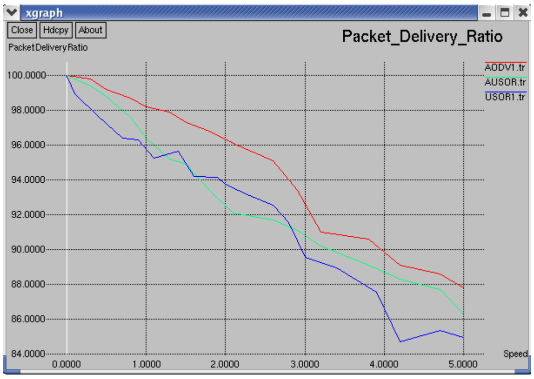


Figure 11 Packet Delivery Ratio

In Figure11 the packet deliver ratio between AODV, USOR and modified USOR is calculated. The performance of modified USOR is better than USOR and lesser than AODV but has performance above 80%.

6.2. Packet Delivery Delay

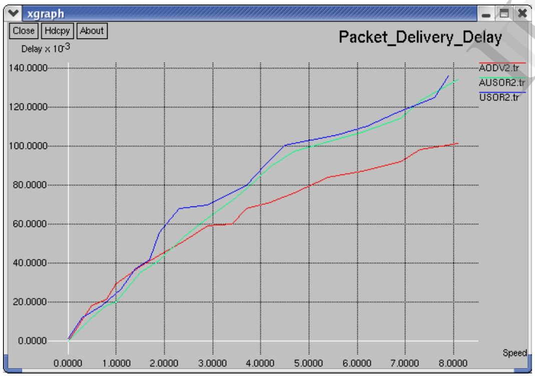


Figure 12 Packet Delivery Delay

In Figure12 the packet deliver delay between AODV, USOR and modified USOR is calculated. The delay of modified USOR is lesser than USOR and higher than AODV.

7. Conclusion

Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. USOR is an Unobservable Secure On-demand Routing protocol for mobile ad hoc network that achieves unlinkability and unobservability by employing anonymous key establishment based on group signature. There is no security provision against the wormhole and black hole attacks in existing USOR protocol. In modified USOR four types of attacks including Selfish node attack, Flooding attack, Wormhole attack and Black hole attack are dealt. AODV, USOR and modified USOR are implemented on ns2 and their performances are evaluated. The security analysis demonstrates that Modified USOR not only provides strong privacy protection, but it is also resistant against attacks due to malicious node and its performance is better compared to USOR.

8. Future Work

In future the nodes causing denial of service attacks should be detected and making USOR a secure quality of service (QoS) aware routing protocol. Along with this the speed of the mobile nodes can be improved and the performance can be analyzed.

9. References

[1] Kui Ren, Ming Gu, and Zhiguo Wan (2012) “USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks” *IEEE Trans. on Wireless Communications*, vol. 11, no. 5, pp. 1922-1932.

[2] Adrian Perrig, David B. Johnson and Yih-Chun Hu (2006) "Wormhole Attacks in Wireless Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2.

[3] Bao F, Deng R.H, KankanHalli M, Wan Z. and Zhu B. (2004) “Anonymous Secure Routing In Mobile Ad-Hoc Networks,” in *IEEE Conference on Local Computer Networks*, pp. 102–108.

[4] Boukerche A, El-Khatib K, Korba L. and Xu L. (2004) “SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless And Mobile Ad Hoc Networks,” in *IEEE LCN*, pp. 618–624.

[5] Buttyan L, Capkun S, and Hubaux J. (2003) “Self-organized public-key management for mobile ad hoc networks,” *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64.

[6] Chim T.M, Dong Y, Hui C.K, Li V.O.K. and Yiu S.M. (2009) “ARMR: Anonymous Routing Protocol with Multiple Routes For Communications in Mobile Ad Hoc Networks,” *Ad Hoc Networks*, vol. 7, no. 8, pp. 1536– 1550.

[7] Defrawy K.E. and Tsudik G (2011) “ALARM: Anonymous Location-Aided Routing in Suspicious Manets,” *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358.

[8] Gene Tsudik and Karim El Defrawy, (2011) “Privacy-Preserving Location-Based On-Demand Routing in MANETs,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1926– 1934.

[9] Hong X. and Kong J. (2003) “ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks,” in *Proc. ACM MOBIHOC’ 03*, pp. 291–302.

[10] Korba L, Song L. and Yee G. (2005) “AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks,” in *ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 33– 42.