An on-demand Routing protocol for secure routing and transmission in MANET

Suggu Hemakumar
Maharaj Vijayaram Gajapati Raj College Of Engineering
M.Tech(CNIS)
Vizianagaram
Andhrapradesh

Abstract

Protecting Routing is crucial in mobile adhoc networks. Routing requires better privacy protection. So many routing schemes have been proposed to protect privacy in routing but these schemes offers partial unlinkability and unobservability because the data packets and control packets are still linkable and distinguishable. In this paper, we've got an inclination to stipulate solid secrecy wants about secrecy-maintain routing in MANET. We've got an inclination to propose associate imperceptible secure routing theme An Unobservable secure On-Demand Routing protocol for Mobile Ad Hoc Networks(USOR) to produce complete unlink ability and content un-observability. USOR is economical as a result of it uses a totally distinctive combination of cluster signature and ID-based secret writing for route finding. Security analysis demonstrates that USOR can well defend user privacy against every at intervals and out of doors attackers.

Keywords— Security, MANET, Routing, Un-Observability

1. Introduction

Mobile ad hoc network is a wireless self-configuring network consisting of theoretically infinite number of mobile processor devices temporarily structurally interconnected into a network by any number of wireless connections. They dynamically self-organize in arbitrary and temporary network topologies, that their elements may independently or in groups form adhoc networks. Each MANET device may independently move in any direction and thus, often change its connections to other devices within the network.

Fig. 1.a MANET devices in ARMY

Fig. 1.b MANET in civil application

Fig. 1 MANET Devices

MANET is a network, which is independent network. There is MANET technology used in different application, like military and civil applications. As a result of figureless property, network could also be laid low with attackers. In our paper we are providing security by using anonymity unlinkability and unobservability. Anonymity [3][9][10] was defined [1] means each and every node in the communication must have a unique node. Unlinkability was also defined [1] if two nodes are in communication if one node ask with whom your communicating in future the another node will not say the further communication. Unobservability was defined [1] the communication will happened in secure area show in Fig. 1.a, Fig. 1.b if any node which is not belongs to secure area try to participate in the communication then the unobservability says that it does not allow that node in to the communication. To avoid these security drawback there are several numerous researchers fictional many security strategies like encoding strategies. To improve security here we are using popular two methods, one is RSA algorithm and Sha-1 algorithm. In this project we suggested un-observability by providing protection on request and reply.

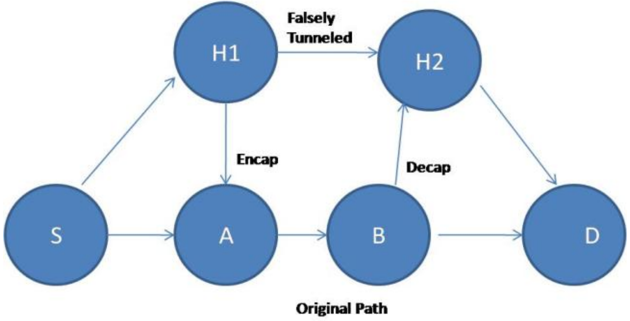

Fig.2 wormhole attack

In a wormhole attack, hackers are tunneled packets to another area of the network bypassing normal transmission routes as shown in Figure 2. In practice, hackers can use eminent power antennas or a wired link, or some other methods. This resulting route through the wormhole may have a meliorate metric, i.e., a lesser hop-count than normal paths. With this purchase, hackers using wormholes can easily fake the routing priority in MANET to perform dropping, packet. The entire routing system in MANET can even be brought down by the wormhole attack.

2. Related Work

ARM [1], author present a novel anonymous on demand routing scheme for MANETs and identify a number of problems of previously proposed works and propose an efficient solution that provides anonymity in a stronger adversary model.

ARM is an anonymous on demand routing scheme for MANETs. In this author first identified a number of problems and strengths in previously proposed solutions and proposed a solution that provides stronger anonymity properties while also solving some of the efficiency problems but the computations are more in this protocol.

SDAR [2], author proposes a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate node.

SDAR is a novel secure distributed anonymous routing protocol for MANET. Author discussed the protocol and highlighted its main features, which include (i) Non-source-based routing (ii) Flexible and reliable route selection, and (3) Resilience against path hijacking. This SDAR use long-term public/private key pairs at each node for anonymous communication. Though these schemes are more scalable to network size but require more computation effort.

ALARM [3], author addresses some interesting issues arising in MANETs by designing an anonymous routing framework (ALARM). It constructs a secure MANET map by using nodes current locations. Based on the current map, each node can decide which other nodes it wants to communicate with.

The ALARM framework is constructed which supports anonymous location-based routing in certain types of suspicious MANETS and it shows that that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high but it mainly relies on group signature.

Dan Boneh, Matthew Franklin [4], author proposes a fully functional identity-based encryption scheme. The performance of the system is comparable to the performance of ElGamal encryption method. The security of the system is based on a natural analogue of the computational Diffie-Hellman assumption.

A cipher text security for identity-based systems is designed and proposed a fully functional IBE system. The system has chosen cipher text security in the random oracle model assuming BDH, a natural analogue of the computational Diffie-Hellman problem but the attacker have some negligible advantage in defeating the semantic security of the system.

Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons,Abraham Flaxman [5], author presents a novel protocol for limiting the corruptive influences of sybil attacks, Sybil Guard. This protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship.

SybilGuard protocol is for limiting the corruptive influences of sybil attacks is proposed, which is mainly used for reducing the sybil attacks of the adversaries on the networks and to provide security to the network but it mainly relies on properties of the users.

3. Problem Description

A number of secure routing outline have been brought forward MASK is based on a special type of public key crypto system and the pairing-based cryptosystems are to achieve anonymous communication in MANET. Existing schemes fail to protect all content of packets from hackers, so that the attacker can obtain data like packet type and sequence numbers etc. These details can be used to relate two packets, which break unlink ability and may lead to source trace back attacks. Another problem of previous outlines is that they rely heavily on public key cryptography and thus incur a very high computation overhead.

4. Proposed System

In this project, we introduced an efficient privacy maintain routing protocol USOR that achieves content un-observability by using anonymous key institution supported cluster signature. This project is implementing high security data transfer so we can avoid hacking unlike data security, it providing the fundamental packet security also.

5. Un-Observability:Algorithm For USOR

In this project we used two different Algorithms. They are RSA and SHA-1. For encrypting and decrypting the message we used RSA algorithm and SHA-1 used for generating the hashes.

We initialize Leader node it can share the key at initial time. Leader node initially sends the Group ID key to all then mobile nodes. If normal node received that ID then stores into memory. If node having GID it can access the request otherwise it can't access the request. If node (i) wants to communicate with another node then node (i) generates the hash code(by sha-1) then the hash code will encrypt (by RSA) with private key of node (i) and then sends to destination node (j). The Destination node can verify that encrypted message by using the public key and as well as group ID. If it matches then node (j) sends own code to source node (i). if public key and group ID is not matched then it simply ignores the transmission of the data.

6. Application Area and Project Description

In Military applications when the soldiers are moving from secure area to insecure area with wireless devices (mobile nodes) there is a chance of getting malicious node in insecure area. In our project we avoid that malicious node when soldiers move to insecure area.

During this project, we have a tendency to outline solid privacy necessities relating to privacy-maintain routing in Manet. We have a tendency to propose associate imperceptible secure routing theme USOR to supply complete unlink ability and content un-observability for every kind of packets. USOR is economical because it uses a completely unique combination of cluster signature and ID-based encoding for route discovery. The simulation results show that USOR not solely has satisfactory performance compared to AODV, however additionally achieves stronger privacy protection than existing schemes like MASK

7. Routing Routes

7.1 Basic Routing Route

If the source has no route to the destination, then source initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination vehicle.

If a closer neighbor node is available, the RREQ packet is forwarded to that vehicle.

If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

A destination node replies to a received RREQ packet with a route reply (RREP) packet in only the following three cases:

1) If the RREQ packet is the first to be received from this source vehicle
2) If the RREQ packet contains a higher source sequence number than the RREQ packet previously responded to by the destination vehicle
3) If the RREQ packet has the same source sequence number as the RREQ packet previously responded to by the destination node, but the new packet indicates that a better quality route is available.

7.2 Include hacking in basic routing Route

In this module we are including the hacking node with our network so the attacking node creates problem. And now we are going to analyze our current network status with some problem and able to solve it.

7.3 Protection against hacking

In this module, we are implementing USOR by protecting all information about that particular packet.
In this module the packet is identified by authorized user's only, other node can't identify information about that packet.

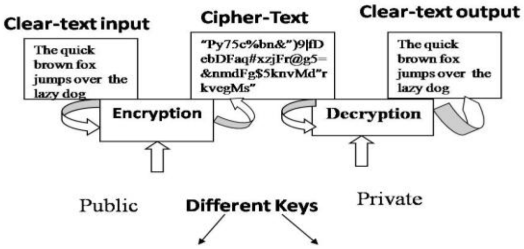
Clear-text input
The quick brown fox jumps over the lazy dog
Cipher-Text
"Py75c%bn&")9|fD ebDFaq#xzjFr@g5= &nmdFg$5knvMd"r kvegMs"
Clear-text output
The quick brown fox jumps over the lazy dog
Encryption
Decryption
Public
Different Keys
Private

Fig.3. Protection against hacking

In this module, we've a bent to implementing USOR by protecting all knowledge that express packet. In this module the packet is thought by approved users exclusively, various nodes can't confirm knowledge that packet. In this we included digital signature method to make more secure transmission. For making Digital sign we can use cryptosystem technique. There are four processes that are specific and essential to a pair wise key cryptosystem:

a) Decrypt an encrypted message gives you the original info, specifically

$$\mathbf{D\ (E\ (M)) = M}$$

b) Reversing the process still returns M:

$$\mathbf{E\ (D\ (M)) = M}$$

c) E and D are simple to compute.

d) The publicity of E does not concede the D secrecy, meaning you cannot simply figure out D from E.

Let e, d, n be positive integers, with (e, n) as the encryption key, (d, n) the decryption key, **n = pq**.

Now, we encrypt the message by raising it to the eth power modulo n to obtain C, the cipher text. We then decrypt C by raising it to the dth power modulo n to obtain M again. Formally, we obtain this encryption and decryption algorithms for E and D:

$$C \equiv E(M) = M^{e} mod(N)$$
$$M \equiv D(C) = M^{d} mod(N)$$

8. Analysis

Network performance refers to the service quality of a communications product as seen by the customer. As each network is different in nature and design there are many different ways to measure the performance of a network,

8.1 Packet delivery function

Packet Delivery Function (PDF) is the term used to measure the network performance. PDF defines the how much packet delivered correctly over total number of packet sent. PDF is analyzed in XGraph on ns2 simulator

8.2 Overhead

Overhead is the one important concept to analyze network performance. Overhead is defined as number of routing and control packet is requiring transferring the data. Overhead is analyzed in XGraph on ns2 simulator

9. Results

In our project, we analyzed different network environment with main network parameters such as packet delivery ratio and overhead. In previous work the researcher tested only black hole attack in our work we tested with worm-hole attack also. From our result USOR providing solid security over worm-hole environment also.

Result shown Fig.4 is packet delivery function, Over head and Delay In that graph, there are the three environments (AODV,Mali,USOR) shown. From our result, we can know we improved our network performance.

TABLE1: PERFORMANCE COMPARISON

Protocol	***PDF (%)***	***OH(pkt)***	***Delay(ms)***
AODV	88.926	306	38
Mali	8.2	305	410
USOR	81	190	39

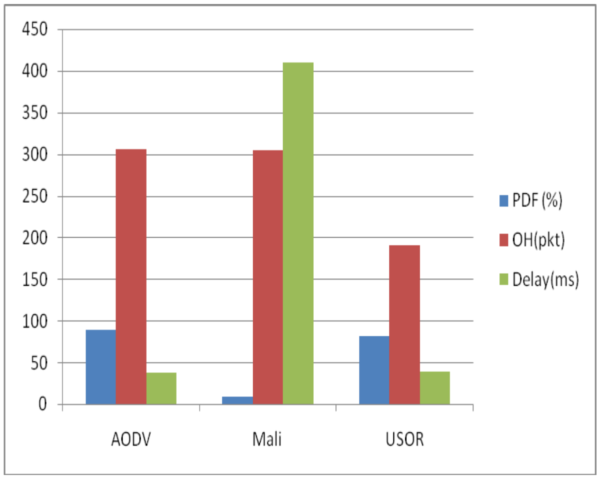

Fig.4. Performance comparison

The Table1 and Fig.4. Above determines PDF of AODV is 88.926 without malicious environment but the PDF of USOR is less than the normal AODV but USOR includes the hacking nodes so it provides the high security compare to normal AODV even though PDF is less. OH, from this result we will grasp USOR has a lot of overhead than traditional AODV. USOR performance is best than traditional AODV even overhead is more; the rationale is security of USOR is extremely high therefore overhead is ignorable during this case.

Result shown Fig.5. Bellow is packet delivery performance. In this graph, there are the 3 atmospheres (without malicious environment, with malicious atmosphere and USOR environment) shown.

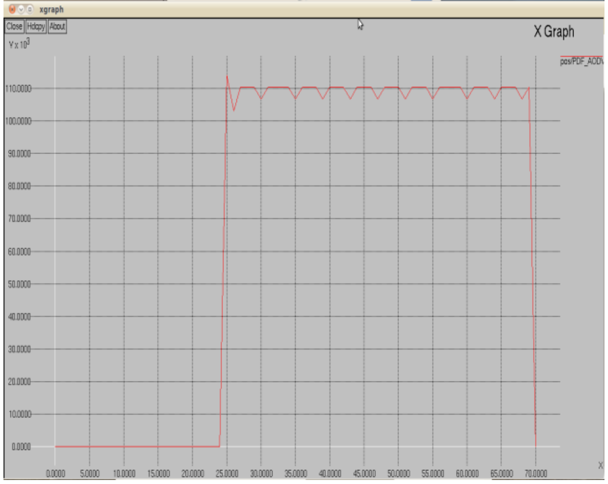

Fig.5 (a).Without malicious environment(AODV)

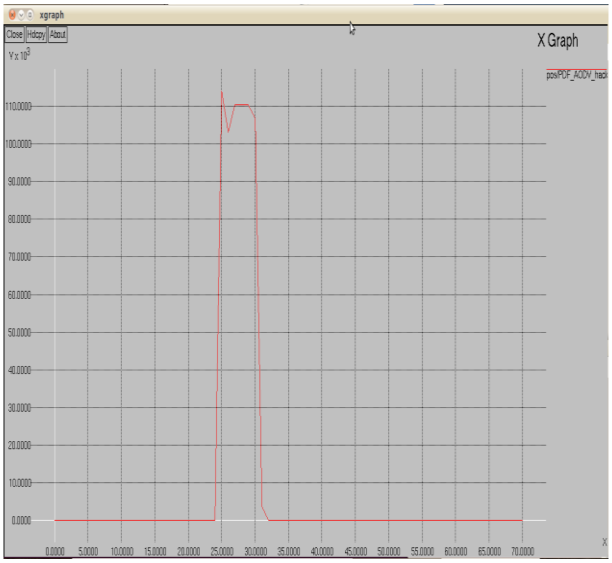

Fig.5 (b).With malicious environment

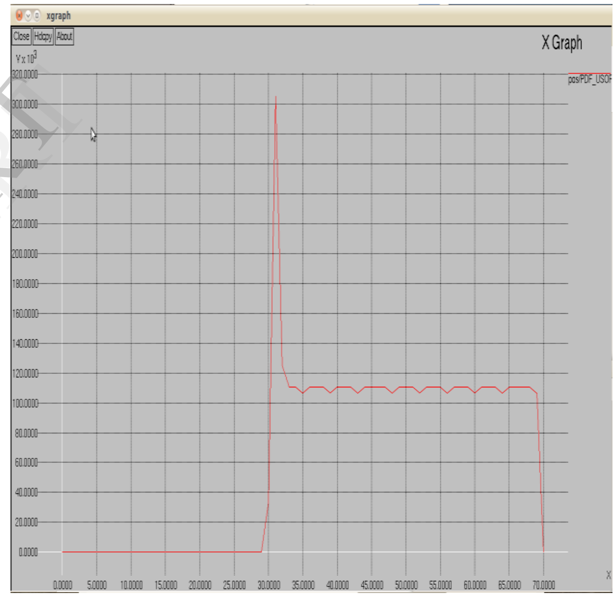

Fig. 5(c).USOR Environment

Fig.5. Packet Delivery Function Comparison b/w AODV, Mali_AODV and USOR

The graph shown Fig.6 is overhead graphs, from this result we will grasp Fig.6(c) has a lot of overhead than traditional AODV show in Fig.6.(a).AODV . Fig.6(c).USOR performance is best than traditional AODV even overhead is more; the rationale is security of USOR is extremely high therefore overhead is ignorable during this case.

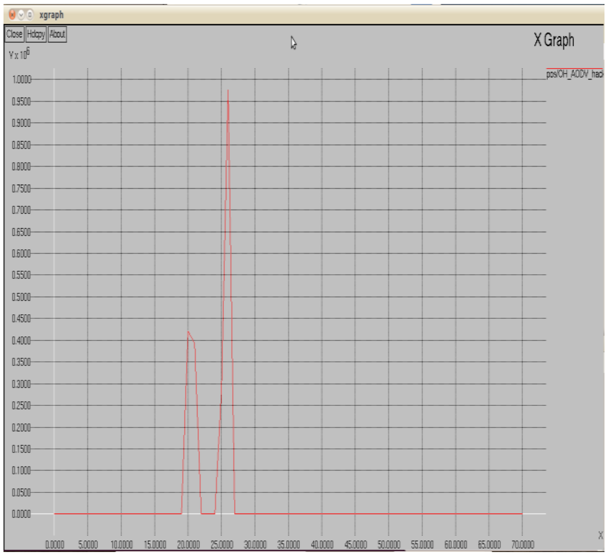

Fig.6.(a).AODV

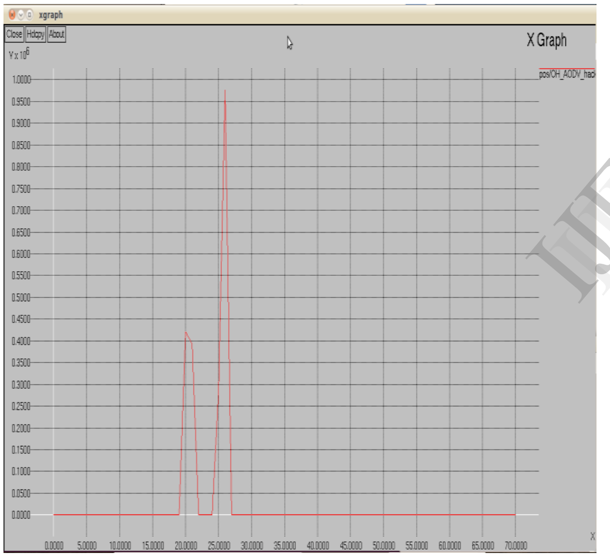

Fig.6(b).Mali AODV

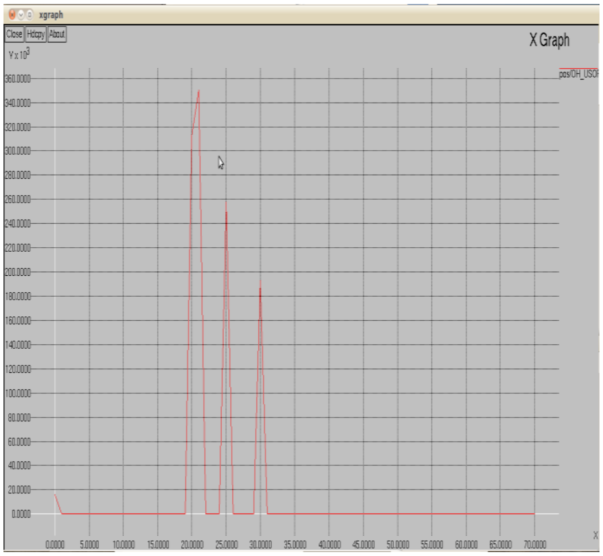

Fig.6(c).USOR

Fig.6 . Over Head Comparison b/w AODV, Mali_AODV and USOR

9.1 Simulation setup

We simulate results in ns2 and we consider 50 nodes. We simulate mobile adhoc network with 46 normal nodes and 4 malicious nodes. We set the nodes to move some distance. The topology is simulated in the space of 1400 dimension on X axis and 1400 dimension on Y axis. Initially we set channel as a wireless, propagation as a TwoRayGround, Antenna as OmniAntenna. By default we set routing protocol as a AODV and the total simulation time will be 70 seconds. in this time the transmissions between the node to node will be secure.

10. Conclusion & Future Work

In this paper, we have a tendency to prompt associate imperceptible routing protocol USOR supported cluster signature and ID-based cryptosystem for impromptu networks. The conception of USOR offers solid privacy protection complete unlinkability and content unobservability for impromptu networks. The protection analysis demonstrates that USOR not solely provides robust privacy protection , it's additionally a lot of resistant against attacks as a result of node compromise. We tested successfully worm-hole attack in our method. In our project the group ID is static so for the future work it can be dynamic so that we can provide more security.

11. Acknowledgement

We wish to acknowledge the help of ***Mr Veerabadra Rao., Associate Professor,*** for guidance which helped us work hard towards producing this research project work.

References

[1] Stefaan Seys and Bart Preneel "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks", International Journal of Wireless and Mobile Computing , Volume 3 Issue 3, October 2009 , pp. 145-155

[2] Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba. "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks", Local Computer Networks,. 29th Annual IEEE International Conference on 16-18 Nov. 2004, pp. 618 – 624

[3] Karim El Defrawy and Gene Tsudik. "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", Mobile Computing, IEEE Transactions , Volume:10, Sept. 2011, pp. 1345 - 1358

[4] Dan Boneh, Matthew Franklin. "Identity-Based Encryption from the Weil Pairing", CRYPTO '01, Volume 2139, 2001, pp. 213-229

[5] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons,Abraham Flaxman."SybilGuard: Defending Against Sybil Attacks via Social Networks", Networking, IEEE/ACM Transactions , Volume: 16, June 2008 , pp. 576 - 589

[6] Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao. "On Flow Correlation Attacks and Countermeasures in Mix Networks", Privacy Enhancing Technologies ,2004,pp. 207-225

[7] Yanchao Zhang, Wei Liu and Wenjing Lou."Anonymous Communications in Mobile Ad Hoc Networks", ICUCT 2006 , Volume 4412 , 2006, pp 140-149

[8] Srdjan Capkun, Levente Butty ́ n and Jean -Pierre Hubaux."Self-Organized Public-Key Management for Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Volume 2, 2003, pp. 52-64

[9] Jiejun Kong, Xiaoyan Hong. "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks", ACM international symposium on Mobile ad hoc networking & computing, 2003, pp 291-302

[10] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H.Deng."Anonymous Secure Routing in Mobile Ad-Hoc Networks", IEEE International Conference on Local Computer Networks, 2004, pp. 102-108

[11**]** Gianni Di Caro*,Frederick Ducatelle, Luca Maria Gambardella "An Adaptive Nature-inspired Algorithm for Routing in mobile ad hoc networks" ,Volume 16 , 2005,pp. 443–455,

[12] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks", IEEE transactions on parallel and Distributed Systems ,Volume 24,2013,pp.239-249

[13] Zhiguo Wan, Kui Ren, and Ming Gu "An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Transactions on Wireless Communications, Volume. 11, 2012, pp. 1922-1932

[14] Wei Liu , Hiroki Nishiyama , Nirwan Ansari , Nei Kato "A Study on Certificate Revocation in Mobile Ad Hoc Networks", IEEE Communications Society, ICC 2011