Lightweight Energy Proficient Anonymous Routing for Low-power MANET

A.Naveena,
Assistant Professor, ETM dept,
GNITS,
Hyderabad, INDIA.

Dr. K.Rama Linga Reddy,
Professor and HOD, ETM dept,
GNITS,
Hyderabad, INDIA.

***Abstract*— Low-power Ad Hoc systems are the most challenging aspect for secured Ad Hoc systems. The resource constrained devices were easily tampered due to the limited operated environment. Over the past decade, the usage rate of Ad Hoc systems are rapidly increased in modern communication systems. However, the security is still a research factor for Low-power Ad Hoc systems. Offering Security and Anonymity is an important research issue in Low-power Mobile Ad Hoc Networks (LPMANET). Various anonymous routing protocols presented to maintain anonymity in adverse environment, these protocols proven significant results in Ad Hoc systems but failure to improved the anonymity efficiency in Low-power Ad hoc networks. In this paper, a Lightweight Energy Efficient Anonymous Routing (LEEAR) protocol is proposed to offer energy efficient anonymity and security in an adverse environment by combining modified zero knowledge proof, bloom filter and cryptography techniques. We designed the LEEAR protocol to determine the efficiency in-terms security and energy against routing level and traffic level attacks. We simulated the experiment in NS2 simulator the determine the results and ensure importance of the proposed LEEAR protocol in accomplishing energy efficiency and anonymity**

Keywords - Mobile Ad Hoc Networks, anonymity, pseudonymity, ZKP, Bloom fiter, ECC

I. INTRODUCTION

Ad-hoc networks are self maintained networks which can dynamically organize network topologies without any centralized resource.. Many secured routing protocols were proposed to provide privacy to the nodes but could not maintain performance efficiency. a node to maintain its privacy, it should implement anonymous routing protocols [1], [2], [3], [4].These anonymous routing protocols should also prevent adversaries like broadcast attacks, traffic analysis.

After deep observation about these protocols, the Anonymous Location-Aided Routing in MANETs (ALARM)[8] provides secured communication against adversaries by dealing node anonymity and integrity. But failed to protect anonymity with regard to location of source and destination.

In-order to protect location anonymity, Haiying Shen [5], proposed An Anonymous Location-Based Efficient Routing Protocol (ALERT) [5]. In this protocol, the network is partitioned such that source node and destination node are in different zones but failed to provide node authentication. In order to maintain efficient anonymity, the AASR [6] protocol proposed key-encrypted onion and group signature for maintaining anonymity in a network for providing on-demand security. However the AASR didn't balance energy due to the lack of cryptographic computations and secured routing process. In addition most of these protocols organize secured routing with less delay performance. These routing protocols are limited in-terms of energy efficiency and pseudonymity.

This paper presents lightweight energy efficient anonymous routing protocol by combining the zero knowledge proof, bloom filter and Elliptic curve cryptography techniques to achieve energy efficiency and security. In this paper, we modified the zero knowledge proof and encrypted the node identity with bloom filter and ECC [14]. The paper is described discusses related work in Section II, , background and System Model in Section – III, proposed model in Section – IV, Protocol evaluation in Section – V, Performance evaluation in Section VI and Conclusions in Section VII.

II. RELATED WORK

TABLE I. ANONYMOUS ROUTING PROTOCOLS

Techniques	Advantages	Disadvantages
Anonymous On-Demand Routing (ANODR) [9]	ANODR uses one time public and private key to achieve anonymity in MANET.	The ANDOR failed to achieve guarantee content un-observability
Anonymous Location-based and Efficient Routing protocol (ALERT) [5]	ALERT organizes a network into zones, it chooses random node as a relay node to maintain anonymity by forming a non raceable anonymous route.	This protocol organizes the similar groups in a network, if any one of the node is dishonest the whole group is considered as a dishonest group
AASR [6]	This protocol uses onion routing to provide	This protocol failed to

978-1-5090-1560-3/17 $31.00 © 2017 IEEE
DOI 10.1109/IACC.2017.72

	anonymity	achieve better end to end delay.
Anonymous On-Demand Routing (MASK) [10]	MASK encrypts and decrypts packets at each hop based on the shared secret of each pair of adjacent nodes.	This scheme does not provide destination anonymity.
Authenticated Key Exchange for Wireless Ad Hoc Networks [11]	. The proposed protocol uses an efficient ring signature scheme based on ECC to achieve anonymous authenticated key agreement among mobile nodes in the network.	In this scheme the network produces more routing packets to identify the route, it causes routing overhead and network suffers from route message flooding
On-Demand Lightweight Anonymous Routing [12]	This scheme applies anonymity based on the properties of polynomial interpolation compared to cryptographic approach mechanism. The traditional polynomial interpolation consumes less computational energy.	The secret sharing scheme is not much efficient due to the lack of poor polynomial computations. In addition it increases End-to-End delay

III. BACK GROUND AND SYSTEM MODEL

This section comprises of a brief description about network model, adversary model, bloom filter and zero knowledge proof which are implemented in our proposed model.

A. Network Model

We consider multihop mobile ad-hoc network model consisting of number of mobile nodes, which are represented with dynamic mobility. Nodes are dynamically distributed and the network is modeled as $G(N,R)$, where N represents set of nodes and R represents set of routes for set of pairs (n_i, n_j), the node n_i forms a routing towards node n_j with the help of neighbor nodes n_k. The routing is not stationary, it dynamically changes with corresponding available nodes n_k . The neighbor nodes n_k forward data towards destination n_j. The node n_i generates anonymous RREQ message in a network to discover a route to protect node identity and the neighbor nodes n_k form a trusted environment to protect a sender node against routing attacks.

B. Adversary Model

MANETs are easily compromised with attacks due to its mobility and resource constrained nature. Generally mobile nodes have less security infrastructure and low data preserving factors, where data communication is not highly reliable. The attacks are classified as passive attacks and active attacks [1]. The passive attacks eavesdrop the packets to analyze the traffic and it identifies the critical nodes to pin point as active attacks. In this paper we consider passive and active attacks and we analyze both the attacks to ensure secure communication.

C. Bloom Filter

A Bloom filter with a set of items $S=\{S_1, S_2, S_3....S_n\}$, with an array of n bits and m independent hash functions $h_i=\{h_1, h_2, h_3....h_n\}$ with range $\{1,.....m\}$, hash functions h_i maps item uniformly in a specified range is used. Each item $S_i \in S$ the bits at the positions $h_1(S), h_2(S), h_3(S)....h_m(S)$ in a vector n. Bloom filter can be represented as $b_i=\{b_1, b_2, b_3....b_m\}$. To add item S into BF, item S is hashed with m hash functions. The bits corresponding to these hash values are set 1 in a bit array. To enquiry the membership of an item $s \in S$, the bits at indices $h_i(S)$ are verified. If any of the value is 0 then the conviction $s \notin S$. Then the values are set to 1 with higher probability. In this paper we use bloom filter for identifying route loops.

D. Modified Zero knowledge Proof with Trapdoor

Goldwasser, Micali, and Rackoff have introduced the basic notation about Zero-Knowledge Proof [13] in 1985. Zero-Knowledge (ZK) proof is an illustration of interactive proof protocol. An interactive proof protocol is one that authenticates a prover to a verifier using challenge-response mechanism. In this mechanism, the verifier can accept or reject the prover at the end of their communication. In this kind of the system the "prover" can prove ownership of a certain piece of information to a "verifier" without revealing it.

In cryptography system zero knowledge proof is a one kind of authentication system where a prover is able to convince the verifier that it knows the secret without revealing any information of the secret itself. We modify the ZKP to implement in anonymous routing protocols where the destination verify that it is the destined recipient, while other nodes can not learn anything about the identity of the destination

Definition 1: In ZKP system for input a in set of information S, witness w, and the key generator, prover and verifier defined as

Key generator: $\sigma \leftarrow key(1^k)$ *which generators random public string* (1)

Prover : $p \leftarrow P(\sigma,a,w)$ *produces proof* (2)

Verifier v: $V(\sigma,a,p)$ *accepts or reject the proof* (3)

The objective of the ZKP is to satisfy the completeness and non-adaptive soundness

Definition 2: Completeness

$\forall a \in S \in R(a) : Pr[\sigma \leftarrow key(1^k); p \leftarrow P(\sigma,a,w):V(\sigma,a,p)=1] = -(key)$ (4)

Definition 3: Non-adaptive soundness

$\forall a \notin S: Pr[\sigma \leftarrow key(1^k); \exists p : (a,\sigma,p) =1] = -(key)$ (5)

The main idea of non-adaptive soundness system is to prevent the proverb to cheat verifier and

Definition 4: Trapdoor function:

The source random secrete message $a = r^2 |n|$ where n is number of processes.

The source uses open identity in RREQ message to the destination; the open identity computation is derived as

$W_d = \prod_{i=1}^{n} d_s |n|$ (6)

Secret identity: $s_t = r\ W_d |n|$ (7)

Destination Verification: If any node N receives the RREQ packet the node computes W_c its secrete identity

$W_c = \prod_{i=1}^{n} d_i |n|$

Verification: $a = s^2 W_c^2 |n|$

If it matches then it is considered as destination or else node is a not a destination.

IV. PROPOSED MODEL

In this section we are discussing about lightweight anonymous privacy preserving routing protocol proposed.The proposed scheme is categorized into two different phases. First one is anonymous route discovery phase and second is secure data transfer phase. In first phase i.e. the route discovery phase we use modified zero knowledge proof to discover destination and neighbor nodes.

TABLE II. NOTATIONS FOR SECURITY PRIMITIVES

RREQ	Route Request
sequnum	Sequence number
$h(k_n)$	shared session key
En_K	Encrypted session key
$En_{d_{pk}}$	Destination encrypted public key
Ide_d	Destination node identity
$Sesk$	Shared session key
$En_{k_f}(sqno)$	Encrypted symmetric key
$Ps_{s,i}$	Public key of shared session key between sender node to neighbor node
K_f	source node generate symmetric key
APK	Anonymous public key
$RREP$	Route reply
tra_d	Trapdoor constructed by source node
$K_{x,x+1}$	A symmetric key generated by node X and used by node X and X+1.

A. Route Discovery:

The source node S sends RREQ message to communicate with the destination D, if the destination is within a transmission range the source doesn't need to depend upon any neighbor node, if not the neighbor node N should contribute. In this phase there is no public key and session key operations before the route discover. Route discovery process is defined in different phases. In first phase the proposed model represents message type, RREQ, message id and sequence number. In second phase the shared session keys are defined with one way hash functions. We compute hash function with the help of bloom filter and the shared session key are h(k1), h(k2),….., h(kn). The source node uses these shared session keys with other nodes. The node forwards the RREQ message and it may use this established shared session key in other route discovery phase. The advantage of this process is that the source node need not recompute the session keys to ensure the node verifications. The source node uses Anonymous public key (APK), which is a general public key, where some of the nodes know about APK but the nodes can't identify whom it belong to. This key is also used in the RREP phase.

The third phase is to verify the real destination by verifying En_k the encrypted session key message, whether it comes from real destination or not, which is used in RREP phase. We use Elliptic curve cryptograph to organize encrypted session key. The final phase contains $En_{d_{pk}}(Ide_d, Sesk, K_f)$, where Ide_d destination identity, $Sesk$ is shared session key between nodes and K_f source node generate symmetric key. These are all encrypted with destination encrypted pubic key.

The $RREQ$ format is defined as follows

$$S_{rreq} = \{RREQ.sqno\}, \{\{h(k_1), h(k_2), \ldots\ldots h(k_n)\}, APK, tra_d\}, \{En_{k_f}(sqno)\}, \{En_{d_{pk}}(Ide_d, Sesk, K_f), En_{sk}(Mes)\}$$ (8)

Whenever the source node S sends a route request the following route discovery process is described :

1) Check the route request if it was already sent by some other node by using sqno, if it is then drop the request or else process the request
2) If any neighbor node receives request save the REQ message and replace {{$h(k_1)$, $h(k_2)$,….. $h(k_n)$}, APK, tra_d }in new RREQ.
3) Check the shared session key with a neighbor node by comparing $h(k_1)$, $h(k_2)$ in a session key table, if it finds a shared session key then it stores the sqno and $En_{k_f}(sqno)$ to its routing table.
4) Save the APK_x, sqno and $En_{k_f}(sqno)$ as a routing information in routing table.

B. Route Reply Phase:

In this phase the destination D reply to the node N for corresponding RREQ message in following steps

1) When the destination node receives a RREQ , it extracts the corresponding details of $En_{d_{pk}}$ and obtains the ID_{src} by using SK and source signature message to verify node authentication by ensuring $ID_{src,,}$ ID_{dest} , shared key, session key and trap door.
2) If a Destination node D already shared session key with its original source node, the RREP message format is defined as $< ORREP, N_x, E_{k_x}(sqn, K_f) >$. where ORREP is the second part of the message is a pseudonym , E_{k_x} corresponding shared key, Nx is a corresponding pseudonym. It doesn't require to establish new shared key which is an advantage to save energy
3) Then the destination node sends a route reply message if it is a neighbor node receives a message, then the node retrieves the corresponding shared key from routing table generates new RREP at that node and perform this following operation
4) Node X finds $K_{x,\ x+1}$ in its routing table with pseudonyms which comes from the RREP message, then decrypts the third part of the RREP message and gets sqno and shared key $< ORREP, N_x, E_{k_x}(sqn, K_f) >$
5) If not, node X uses the sqno to find the anonymous public key, APK, the new RREP message is constructed as follows $< SRREP, K_{x,x-1}, N_x, E_{APK_{x,x+1}}(sqn, K_f) >$ In which, $K_{x,x-1}, N_x$ are generated by node X, and node X saves them in its routing table.
6) Message is broadcasted.
7) Corresponding node anonymous public key is obtained by node X from the private key by decrypting the RREP.

C. Data Transfer Phase

Once the anonymous route discovery represented the nodes willing to share a data, in this phase the data transfer takes to achieve the confidentiality. The following process is summarized to achieve the data confidentiality. The data transfer phase in LEEAR protocol represents pseudonymity and along with shared key between nodes, where the pseudonym is generated between source node S to other node N. The message is encrypted with Elliptic curve cryptography and shared keys are binded to the encrypted message. The following procedure describes the data transfer

Source transfer the data to the node: $< Ps_{s,t}, E_{K_{s,t}}(Ps'_{t,d}, E_{K_{t,d}}(message)) >$

The source node S transfer a data to the next node with $Ps_{s,t}$, and shared key of source to next node $K_{s,t}$, once the other node N receives a data it verifies the pseudonym in a routing table, obtains a session key for it and regenerate new shared key and encrypts the message updates into the routing table then shares a data to a destination D in anonymous routing path.

V. PROTOCOL EVALUATION

The main objective of this protocol is to achieve energy efficiency and anonymity. We observe this protocol on different circumstances. We consider energy and security parameters to determine the efficiency, although the proposed network model can organize anonymity in any kind of networks. We summarize the protocol efficiency interms of energy level, security level and anonymity level.

A. Energy Efficiency:

The main concern of this protocol is to reduce energy consumption during producing key operation, key validations and control packets. However, this protocol represents anonymous private key and shared session key between nodes to decrypt the packets, if there is already shared session key between nodes then it doesn't required to regenerate new shared session key, in addition the anonymous public key reduces the public key generation operations. In most of the existing anonymous routing protocols such as MASK [10], SDAR[7], they used most of the control packets in anonymous route discovery process, but in our routing protocol don't require any preprocess approach for anonymous route discovery. Generally the control packets consume more amount of energy. Here we are not organizing any prior control packets, hence energy is saved.

A. Anonymity and security

In this protocol, we are efficiently dealing with anonymity and security in different levels. This protocol encrypts the ID's of source node and destination node by employing MZKTP, where destination open identity is protected with trapdoor. The adversaries can't analyze the nodes ID's. In addition this protocol represents pseudonyms to neighbour nodes. These pseudonyms are regularly updated in route establishment phase and data transfer phase so that the malicious node can't trace the real identity of neighbour node.

The anonymous level of proposed routing protocol can well defend the DoS attack, against sending fake routing packets. The proposed protocol mitigates these fake routing packets in anonymous authentication phase. If attacker sends any fake routing packets the forwarder node verifies the encrypted symmetric key sequence number of sender with corresponding encrypted sequence numbers, based on this

instance it can reject the fake routings. In addition this protocol maintains sqno where the reply attacks can't forge the sqno, the reply attack need to reply to the RREQ packet in route reverse phase.

VI. PERFORMANCE EVALUATION

In this paper, we simulate the ad-hoc network model and we compare with various anonymous on-demand routing protocols. We simulate the proposed protocol on following scenarios: Energy Consumption, Network Overhead, Packet Deliver ratio, and End to End delay. We conducted different simulations to obtain results by varying mobility and number of nodes and compared this protocol with AASR and SDAR.

A. Simulation Model :

The experiment is based on ns-2 [15].We have two different simulation models, one is varying node model and another varying mobility model.

In the simulation scenario an ad hoc network of size 1000m × 1000m consists of 50,100,150 and 200 mobile nodes. We configure LEEAR protocol in ns-2 by configuring security packet and routing packet with the network setup features. In this experiment we setup attacker nodes, normal nodes. We simulate this experiment by varying node mobility speed with the rate of 5 to 25ms. In such circumstances the proposed protocol ensures anonymous path by ensuring node identity. The proposed protocol implements the MZKP, bloom filter and elliptic curve cryptography group, the network produces different traffic on different paths, where the protocol ensures the secured data communication by organizing pseudonyms within the nodes.

B. Simulation Results

The performance of LEEAR protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, end to end delay, throughput and energy consumption. Simulation results demonstrate the comparison performance of LEEAR, AASR and SDAR by varying number of nodes and speed.

According to Fig. 1(a), LEEAR have less energy consumption than AASR and SDAR under the different mobile speeds such as 5 to 25 m/s. The energy consumption is 21% less than these two protocols. The Fig 1(b) presents the performance of these protocols, in this scenario we compared the results by varying number of nodes and we determine the energy efficiency by plotting the results. As per the results the energy consumption performance is almost 19% less compare to AASR and SDAR.

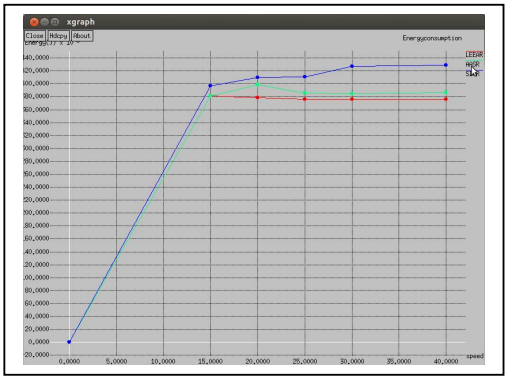

Fig 1(a) : Energy Consumption vs Speed

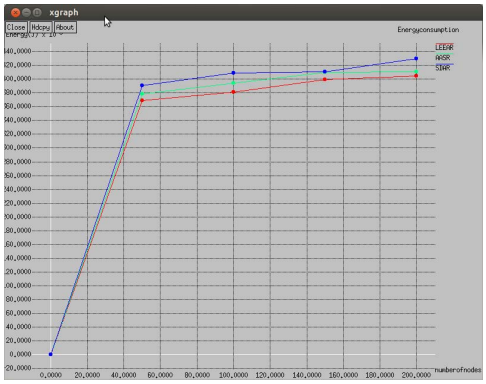

Fig 1(b) : Energy Consumption vs Speed

In other case we compare these protocols by experimenting network overhead. While organizing anonymous routing, the corresponding protocols produce more routing packets which it leads to more overhead to the network. Based on the simulation results the Fig 2(a), presents the network overhead of LEEAR have better packet delivery ratio than SDAR [7] and AASR [6] under different mobile speed and network models. The difference between LEEAR protocol and AASR on packet delivery ratio is less than 6% and for SDAR is less than 8%.

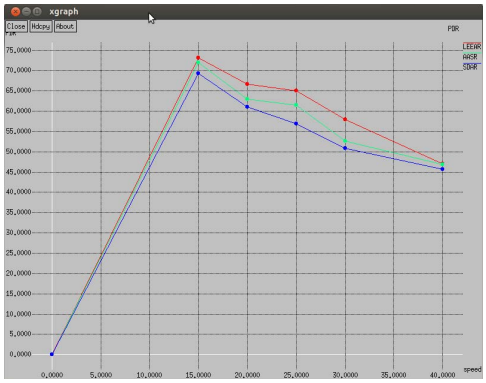

Fig 2(a) PDR vs. Speed

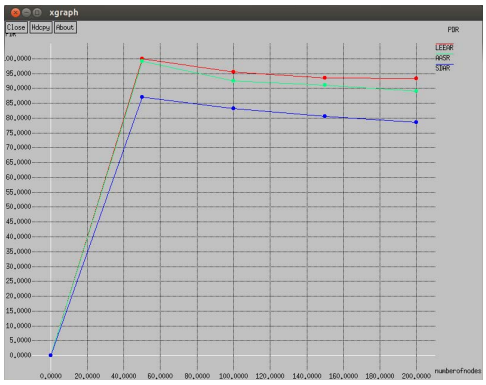

Fig 2(b) PDR vs. No of nodes

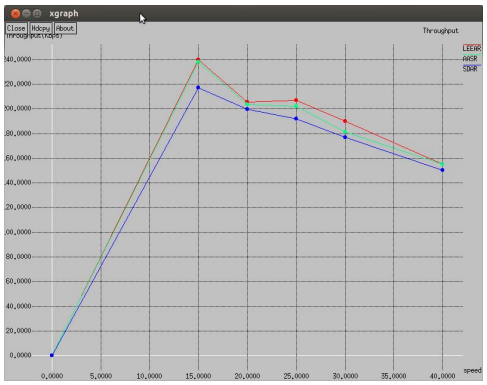

Fig 3(a) : Throughput vs Speed

Comparison of throughput and end to end delay performance for the three protocols is shown in the Fig 3(a) and Fig 4(a) by varying the speed.

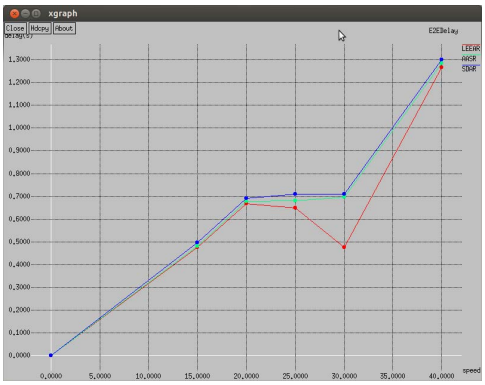

Fig 4(a) E2E Delay vs Speed

VII. CONCLUSION

In this paper, we have proposed the design of an energy efficient anonymous routing protocol for low power MANETs. Anonymous routing and data transfer by reducing key generation and control packet overhead is achieved. In this protocol we achieved energy efficiency and security by reducing public keys and as well as control packets. We compared the performance with other anonymous routing protocols such as SDAR and AASR. Based on simulation results the proposed protocol achieves better energy efficiency and ensured the anonymity against routing attacks.

In our future work, we can include trust model to achieve better link failure detection, which is caused either by adversarial attacks or by mobility.

REFERENCES

[1] Yanchao Zhang; Wei Liu; Wenjing Lou; "Anonymous communications in mobile ad hoc networks "INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE Volume 3, 13-17 March 2005 Page(s):1940 -1951 vol. 3

[2] Jacobsson, M.; Niemegeers, I.; "Privacy and Anonymity in Personal Networks " Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on 8-12 March 2005 Page(s):130 - 135

[3] F. D¨otzer, "Privacy issues in vehicular ad hoc networks," in Proc. of the Workshop on Privacy Enhancing Technologies (PET), 2005.

[4] Giuseppe Ateniese, Jan Camenisch, Breno de Medeiros "Untraceable RFID Tags via Insubvertible Encryption" Proceedings of the 12th ACM conference on Computer and communications security CCS '05 November 2005, ACM Press

[5] Haiying Shen, Member, and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013

[6] Wei Liu, Member, and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 9, NOVEMBER 2014

[7] A. Boukerche, K. EI-Khatib, L. Xu, and L. Korba. "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Network", The 29th Annual IEEE International Conference on Local Computer Networks, Tampa, Florida, USA, 2004 .

[8] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, Sep. 2011

[9] J. Kong, and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks," in Proc. 4th International Symposium on Mobile Ad Hoc Networking & Computing, New York, 2003, pp. 291-302.

[10] Yanchao Zhang, Wei Liu and ,Wenjing Lou, "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 9, SEPTEMBER 2006

[11] L. Xiaodong, L. Rongxing, Z. Haojin, H. Pin-Han, S. Xuemin, and C. Zhenfu, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks," in Proc. IEEE International Conference on Communications, Glasgow, 2007, pp. 1247-1253.

[12] Q. Yang, H. Dijiang, and K. Vinayak, "OLAR: On-demand Lightweight Anonymous Routing in MANETs," in Proc. 4th InternationalConference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.

[13] Goldwasser,S.,S.Micali and C.Rackoff. "Knowledge Complexity of Interactive Proof Systems", Proceedings of STOC 1985, PP. 291-304

[14] D. Johnson, and A. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Technical Report CORR 99-34, Centre for Applied Cryptographic Research (CACR), University of Waterloo, 1999.

[15] Network Simulator: http:///www.isi.edu/nsnam/ns