Anonymous Routing Protocols in MANETs, a Security Comparative Analysis

Ayman M. El-Zoghby
Nile University
Cairo, Egypt
a.zoghaby@nu.edu.eg

Ahmed Mosharafa
Nile University
Cairo, Egypt
ahmedmosharafa@gmail.com

Marianne A. Azer
National Telecommunications Institute
Nile University
Cairo, Egypt
mazer@nu.edu.eg

***Abstract*— A Mobile Ad Hoc Network (MANET) is considered a type of network which is wireless and has no fixed infrastructure composed of a set if nodes in self organized fashion which are randomly, frequently and unpredictably mobile. MANETs can be applied in both military and civil environments ones because of its numerous applications. This is due to their special characteristics and self-configuration capability. This is due to its dynamic nature, lack of fixed infrastructure, and the no need of being centrally managed; a special type of routing protocols such as Anonymous routing protocols are needed to hide the identifiable information of communicating parties, while preserving the communication secrecy. This paper provides an examination of a comprehensive list of anonymous routing protocols in MANET, focusing their security and performance capabilities.**

General Terms- MANETs;private routing protocols; anonymous routing.

Keywords— MANETs; efficiency; privacy; security; wireless; and anonymity

I. INTRODUCTION

MANET are being considered a mobile wireless network which represents the underlying infrastructure for the mobile networks that serves a special time or mission critical applications . Some of the MANETs characteristics such as transmission and mobility of the nodes subject the network to different types of security attacks [1].

The threat model for MANET attacks can be divided into two types, attacks of a passive nature and attacks of an active nature. In the first type, the attacker doesn't interfere with the communication, however he taps into the communication between two nodes trying to sniff or listen to the on-going communication, thus posing serious threat to communication privacy. Passive attacks are highly stealthy and undetectable, which increase their impact. Active attacks can be done either by injecting or modifying the communication traffic to alter transmission and gain privilege to spy on the conversation or violate its integrity. Some of the famous attacks include Black-hole, Wormhole, and Gray-hole attacks [9].

The design parameters surveyed for the study are the routing protocols used, route discovery process, route maintenance process, and location-based routing feature. As for the security parameters surveyed; which are cryptographic algorithm used, privacy features, anonymity features and node authentication capabilities. The surveyed protocols are AC-PKR, ALARM, ALERT, ANDOR, ARM, ASR, AO2P, Discount-ANDOR, HANOR, MASK, TARo, RIOMIO, and SDDR.

The categories of the protocols of routing in MANETs are three: Proactive routing (table-driven), Reactive routing (on demand routing), and Hybrid routing [1].

OSLR, DSDV, and TBRF are examples of proactive adhoc routing protocols. In these protocols, the information in the routing messages includes node ID and how other nodes are being connected to that node (via distance vector or link state methods), are being exchanged frequently to allow nodes to function correctly with the most updated network topology. DSR and AODV are examples of reactive routing protocols. As for the hybrid routing protocols, they aggregate the advantages of both LS and DV protocols, by maintaining a proactive routing table for MANET nodes within the range of their predefined routing zones, and use the reactive feature for nodes outside those zones. Examples of the hybrid protocols are Zone Routing Protocol (ZRP) and Fisheye State Routing (FSR) [15].

Anonymous routing protocols became of critical importance to the security of MANETs [1]. In this paper, the security and performance aspects of the current anonymous routing protocol shall be discussed. Each protocol has a distinct operation mode, while they share some common characteristics as it will be clarified. The provisioning of anonymity and privacy features is different in each protocol, in terms of implementation or application. The challenges that those protocols face during usage will also be presented.

This paper is organized as follows. In sections II background and III related work will be presented respectively. In section IV, the routing protocols are compared. Finally, conclusions and future work are presented in section V.

II. BACKGROUND

Good end to end encryption services are provided by the currently used On-Demand anonymous routing protocols, which comprise four phases [6].

1) ***Anonymous neighbour authentication:*** Nodes will share its keys with neighboring nodes, in order of one hop

count, after a trust is created between each node and its neighbor, hence the Route discovery process becomes very fast

2) ***Anonymous route discover***y: Two messages are used in the route discovery process, A)Unicast or Multicast route reply (RREP) message and B)Boradcast route request (RREQ) message

3) ***Anonymous data transmission***:. A (DATA) message sent to the destination while concealing the identity of any nodes in the path between the source and the destination, hence the link information between the both nodes doesn't exist.

4) ***Route maintenance:*** The routes can be maintained by looking for any dropped links by monitoring the keep-alive messages and the lower layer parameters [9]. To detect if a link is broken an (ERROR) message will be sent back to the original sender. To provide a link breakage detection mechanism, the simple (ERROR) message can be used.

The only work done in comparing some of the anonymous routing protocols in terms of performance were by Anupriya et.al in [9]. The covered protocols were AO2P, ALARM and ALERT only.

III. TERMINOLGIES

Some of the terminologies of the techniques utilized by the anonymous routing protocols, which are discussed below, are going to be explained in this section.

Broadcast is that the node broadcasts its public key to the nodes. Trapdoor implies that the function is easy to perform in one way while it's hard on the other way. Accordingly, if the node A has a cryptography equation $F(X)$ it's easy to compute the equation while it's hard to find the inverse $F^{-1}(X)$ without prior knowledge of k.

Onion Cryptographic Technique implies that each node on the path from the sender to the receiver adds a layer of encryption; accordingly, it becomes a layered packet encrypted in layers just like the onion structure.

Anonymity has many definitions; however we here use the definition introduced by Pfitzmann and Hansen [14], which is "the state of being not identifiable within a set of subjects".

IV. DIFFERENT ANONYMOUS ROUTING PROTOCOLS

MANETs by their nature suffer from limited power capacity and bounded processing capabilities. "The current anonymous routing protocols provide increased level of anonymity; however it has serval issues preventing it from being highly scalable protocols" [9], i.e. the number of nodes supported by the protocol, This comes mainly form the communication delays and computational overload which is the by-product of the heavy cryptographic processes used in such protocols. To remediate such side effects, some of the purposed protocol implementation methodologies don't provide anonymity features to provide higher level of performance, or overlook some privacy features such as un-linkability. Some protocols use encryption only for authenticating nodes, while others use it to provide onion-routing features. The discussed anonymous routing protocols that are categorized based on the distinct feature of how they achieve node anonymity, either by using Onion Encryption [9] or Pseudonyms Node method [9].

A. ***Pseudonyms Based Anonymous Routing Protocols***

1) Anonymous Routing Protocol (ARM)

The ARM [7] was proposed to solve the inefficiency found in other anonymous routing protocols, for example in ASR and ANDOR all the forwarding node will produce a new public/private key pair for all the RREQ messages it sends forwards to the other nodes, therefore, the network is flooded with RREQ, also in SDAR as it requires every forwarding node to perform a public key decryption, a public key encryption and a signature generation for every RREQ message it forwards. Furthermore, ARM aims to overcome two different adversaries. [7] There are two possibilities for any attacks, either form internal source, such as internal nodes which can be of malicious intent, hence we can consider each node is a potential attack source. The second possibility is an attack from external source, either an active attack to harm the network by introducing unwanted changes or passive attack to collect information which can compromise the network privacy. This protocol introduces five assumptions, 1) there is a permanent identity for each node that is known to all other nodes which request to connect with the source node. 2) A private key will be shared between the source and destination nodes via (RREQ) message and a list of pseudonyms will be used to identify different sending sources, thus each destination can validate the identity of the sending node. 3) The private key and pseudonyms list will be shared only between limited set of nodes to increase efficiency. 4) The RREP messages will be encrypted with a key which contains the list of all one-hop neighbors of each node and this key will be broadcasted. Seys and Preneel proposed a key management [7] scheme to dynamically implement a key management method which creates new keys for each link and broadcast those keys when a new node joins the neighborhood. 5) A symmetric wireless links are used between all nodes.

ARM security is based on two techniques; Padding and Time-to Live (TTL) which is a mechanism that bounds the lifespan of data in the network, it may be implemented as a counter or timestamp attached in the data, as soon as the given event timespan has ended, the data is discarded. Padding is applied to stop the attacker from knowing the number of hops to the source or destination of the RREQ or RREP messages. This will be defending against external and internal types of attackers. ARM has a probabilistic padding characteristics and TTL scheme, those characteristics prevents the nodes form knowing if the messages they receive come from the original source or any intermediate node. Also, this prevents the nodes forming exactly type of nodes they in the communication path, if it's intermediate node or originating node. The external attacker can know only which nodes sending new messages but can't follow that message nor find its final destination. As

discussed earlier, the TTL scheme used to conceal the real path.

One advantage of this protocol that it's doesn't need to implement a cryptographic function to allow the nodes to discover if the messages are being destined to them or not. Also, the forwarding of RREQ messages by each node only requires a single public key. Only the nodes that happen to be in the path are the ones that need to decrypt and encrypt the message headers using the broadcast keys sent earlier.

2) Anonymous On-Demand Routing in Mobile Ad Hoc Networks (MASK)

MASK [5] creates a trust between a pair of communicating nodes by using Hello messages. Subsequently to discover the different routes, it utilizes two concepts, Pseudonyms and Trust. It conceals the original identity of the communicating nodes although it uses MAC-layer and Network layer messaging [5]. The MASK conceals the identity of senders, receivers, and hides the sender-receiver relationships in addition to node un-locatability. MASK focuses on routing efficiency as well. MASK prevents the leakage of MAC and network addresses information, this may lead to some unwanted drawbacks. MASK uses pseudonyms in a dynamic way rather than static. The authors in [5] claim that MASK ensures node un-locatability and un-trackability, which means that the gathered information by the attackers, such as node IDs or nodes groups will not help them in figuring out which nodes are associated with this information. MASK claims that it provides an end-to-end flow un-traceability, this will prevent the attacker from knowing which neither the original source of the packets or the final destination of them, it even won't enable to know if this packet is part of which communication session. MASK is considered an efficient protocol [5] similar to a classical routing protocol like AODV. The authors claimed that it can mitigate some attacks such as message coding, flow recognition, and timing analysis. MASK has some drawbacks, which are 1) prone to DoS attack against the authentication mechanism on the nodes, by sending overwhelming authentication requests, 2) the routing information in the design mentioned in [5] is protected only from external attackers, because internal nodes can be compromised by internal user and used to sending fake routing information which are difficult to be validated against real nodes [5].

3) RIOMO

With more information available regarding the pseudonym linking used by the protocol, the anonymity of the nodes decreases, a protocol named RIOMO [3] has be introduced to mitigate such risk, by enforcing each node to generate a cryptographic key pair to be used as a node pseudo ID. RIOMO contribute to the reducing the cost of maintaining a pseudo ID for each node, this is done by allowing only the trustworthy node to participate in the routing process. The authentication process of each node with its neighbor makes sure that the authenticated nodes are trustworthy. It provides identity anonymity, location anonymity, route anonymity and robustness. RIOMO adds serval approaches to enforce end-to-end encryption to avoid communication sniffing and traffic analysis.

*B. **Onion Encryption Based Anonymous Routing Protocol***

1) Anonymous On Demand Routing (ANDOR)

ANODR was proposed in [11]. The design depends on "broadcast with trapdoor assignment" concept, the trapdoor concept implies that the broadcasted information is only known to the receiver at the next hop; accordingly, the broadcasted information will be delivered anonymously to those receivers only. This concept applies the onion cryptographic technique mentioned above. ANODR performs symmetric cryptography demanded by public key cryptography system to reduce computational overheads. The protocol performs intrusion detection and route intractability by insuring pseudonymity of the nodes to achieve anonymousness of the sender and receiver nodes identities during exchanging packets. It focuses on two important problems which are the anonymity of the routes and location privacy. ANODR uses pseudonymity to block node attackers and sniffers from uncovering the identity of the transmitting local nodes and from finding Ad-Hoc networks packets defects. Furthermore, it proves that untraceable data forwarding with lack of encryption at the packet header can be easily revealed. The routes are created between the course and destination on demand [11].

2) Discount Annymous on Demand Routing(Discount ANODR)

Discount ANDOR [4] is an improved version of ANODR which provides the same functionality but with lower cost It improves the processing overhead and reduces the communication burdens by lowering the privacy requirements [4]. By using the Discount ANODR the authors demonstrated that source anonymity and routing privacy will be preserved. The intermediate nodes create the path between the unknown source ID and known destination ID [4]. This implies that when an intermediary node receives the packet, it knows nothing about the source but it knows where the destination is. What distinguishes Discount ANODR is that it uses only symmetric key operations making it a lightweight routing protocol while preserving the privacy of the nodes.

The authors [4] assume this protocol is suitable for low-power bounded nodes as it consumes less computational power. The discounted protocol works like this: The node transmitting broadcasts a route request that reaches the destination node. Next step would be the destination node generating a route reply and here is where the encryption happens. Every intermediate node attaches its identity to the received reply; afterwards it chooses a symmetric key to encrypt the packet [4]. Finally, the route becomes cached on the sender node for further communication with the destination node.

3) Hierarchical Anonymous on Demand Routing (HANOR)

HANOR[2] introduces an on-demand routing protocol which is anonymous and hierarchical in nature. It addresses the performance issues that come with the large number of public keys that are used in the current anonymous routing protocols [2]. This routing scheme focuses on data security and guaranteed routing anonymity, either intra-group or inter-group. The hierarchical scheme reduces the cryptographic overhead; which makes it scalable anonymous routing algorithm [2]. The contribution of HANOR is that it takes hierarchical MANET structures into account. During intergroup routing it treats group of nodes as single group to achieve anonymity and route abstraction. The inter-group communication contributes to the reduction of cryptographic overhead which has a negative effect on the power consumption of low-end mobile device; it reduces also the time needed for discovering routes. The authentication process takes place during the route discovery, thus increases the security on the node group level.

4) Anonymous and Certificate-less Public-Key Routing (AC-PKR)

Public key infrastructure (PKI) is a system composed of software and hardware to be used in managing the life cycle of cryptographic certificate. To make sure that public keys generated by the PKI is valid and correct, the PKI systems utilizes certificate authority (CA) component [12]. Using a PKI in a MANET network is cumbersome due to the need of a centralized system to act as a PKI. A certificate-less PKI (AC-PKI) was proposed to be used in Ad-hoc networks. All the complications come from the centralized PKI, such as certificate management and so forth are being eliminated. AC-PKI works as follows [14], if two nodes are to start communicating, the sending node will use the node identifier (IDR) of the receiving node as a public key and generates the cipher test as IBE (IDR, message). IBE is an identity-based encryption function which function is to ensure that the only node which can decrypt the message is the one has the valid private key that corresponds to node's "IDR".

This protocol consists of three main points [14]. 1) a method to security distribute the master encryption key, distributed private key generator (DPKGs), across the pre-selected node, based on Shamir's secret sharing algorithm, this D-PKG has the pre-requisites for the private key-generation (PKG) service. 2) An anonymity protection techniques for the D-PKGs, to prevent pinpoint attacks against certain MANET node. 3) An optimal parameter for the secret-sharing method to ensure highest security measures.

5) Anonymous Location-Based Efficient Routing Protocol(ALERT)

ALERT[8] uses the network zones concept, by grouping randomly chosen nodes in a dynamic way as intermediate relay nodes. This provides anonymous non-traceable route, by making it very hard to attacker to detect which nodes are sender/receiver and which nodes are intermediate [8]. In each routing step, the sending node divide the network into two fields, and create two zone for source and destination nodes, and another zone which has all the relay node to choose from. GPSR routing algorithm is used to send the data to the relay node [8]. The data is then broadcasted to k nodes in the zone of destination node, hence producing k-anonymity to the node of destination. ALERT also conceals the node which initiated the communication within a number of initiators to maximize the anonymity of the sending node. ALERT provides resilient measures against intersection and timing attacks by hiding the identity of the source, routes, and destination routes [8].

C. Trusted Anonymous Routing(TARo)

TARo [6] for MANETs achieves better security and anonymity without compromising the performance requirements [6]. Anonymity is achieved in TARo by utilizing a solution to implement a novel addressing scheme depends on the keyed hash chain [6] by utilizing the Diffie-Hellman one-to-many symmetric key distribution mechanism [6]. Moreover, it verifies the connection between the intermediate nodes to select a trusted route between source and destination. TARo uses the Link Verification Onion (LVO) methods to detect any untrusted routes announcements.

Since most anonymous routing protocol using DH algorithm for the key exchange during the route request phase, this adds the encryption information to the broadcast traffic done by each node. This can adds overhead, however in TARo by avoiding the use of public key cryptography and using symmetric key and hash operations, makes the key exchange and the cryptography process more efficient [6].

1) Anonymous Location-Aided Routing (ALARM)

ALARM [10] provides both privacy and anonymity, by utilizing Link state approach to support its location-based routing, it assumes that the MANET node can obtain a secure location via GPS, has a time-synchronized clock, and at least K number of nodes mobilize in synchronization, while all nodes transmission range are uniform. ALRAM uses Group Signatures, which are essentially public keys that can be verified by anyone inside the network [aka. escrowed anonymity] [10]. Some of the benefits of using group signatures are ensuring that the received "Link Announcement Message" is legitimate, while two pseudonymous nodes would be unlikable. Another feature that can be added to that scheme is "Self-distinction, thus making it possible to detect malicious insider".

ALRAM preserves node privacy across multiple time-slots. The main challenge in ALRAM is how to generate the common parameters that achieves anonymity (i.e. random number). ALRAM also introduced "APN" average node privacy, where it's a metric to indicate to a small part of the overall number of nodes.

V. COMPARISONS

In this section, we compare between the different anonymous protocols that were presented earlier.

A. Mask and RIOMO

What distinguishes RIOMO from MASK is that in MASK, a large number of pseudo IDs are generated, because if a few pseudo IDs are generated, there will be a chance of figuring out a pseudonym link by the attacker. RIOMO can overcome the overhead of network administrator generating pseudo IDs for each node by making the nodes produce and independent and dynamic pseudo IDs.

B. SSDR, ANODR and RIOMO

Secure Distributed routing algorithm (SDDR) is built upon the onion routing protocol, it provides weak location privacy and anonymity for the generated routes, but overlooks the identity anonymity. Regarding the attacks it's immune against the Wormhole and rushing attacks while it's vulnerable to DoS attacks [16].

ANODR (Anonymous on demand routing): ANODR compared with SSDR has more efficiency in the data transmission stage [11]. ANODR doesn't provide identity privacy. SSDR provides the privacy characteristic for both source and destination nodes while ANODR provides the privacy characteristic for only the forwarding nodes. ANODR doesn't provide Strong location privacy as well. However, it provides route anonymity and overcomes the deficiencies of SSDR and ANODR in identity, location and route anonymity. RIMIO is immune against DoS attacks, Wormhole attacks and Rushing attacks.

C. ALERT, AO2P and ALARM

ALERT differentiates form both AO2P and ALARM in providing route, location and identity anonymity for both source nodes and destination nodes; this is due to discarding the hop-by-hop encryption and dependency on redundant traffic. ALERT randomize the routing and increases the node density to maximize anonymity. ALERT transmits data with ow cost and with less latency than the rest of the two protocols, Thus produces low overhead which can benefit MANETs. ALARM saves the node anonymity by authenticating the updates for location changes [9]. ALARM is not tied to only a specific signature scheme; however it can uses any signature scheme to limit attacks from outside and inside attackers [9].

D. SPAAR, MASK, ANODR, D-ANODR, and ARM

These protocols don't use location information for any routing purposes; however they are pseudonyms for identifying the nodes and nodes' addresses [10]. Location-based routing protocols have a goal of providing better performance and low overhead of the protocols used in routing. This performance enhancement comes from controlling the routing messages without flooding the whole network [10].

COMPARISON TABLE

The comparison table below shows the difference features of the selected anonymous routing protocols. The selected features used are mainly security focused to differentiate between these routing protocols in terms of privacy, anonymity, cryptographic strength and route generation.

	ANODR	D-ANODR	HANOR	ALARM	ALERT	ARM	MASK	TARO
Proactive/Reactive	Proactive	Proactive	Proactive	Proactive	Reactive	Proactive	on-demand	On-demand
Location based routing	NO	NO	NO	YES	YES	NO	NO	NO
Cryptography	Symmetric key	Symmetric Key	One way hash function	Group Signature	randomized routing of one message copy	Symmetric Key	Pairing-Based Crypto	Keyed Hash Chain
Origin Authentication	No	No	No	Yes, using Group Signature	No	No	Yes, via secret hand shake	Yes, using DH
Privacy (Node Anonymity)	Use real node identity	Use real node identity	Use real node identity	Doesn't use the real node identity	Doesn't use the real node identity	Use real node identity	Use real node identity	Doesn't use the real node identity

Table 1 (Anonymous Routing Protocol Security Comparison)

Table 1 highlights the differences between the selected routing protocols, which are ANDOR, D-ANODR, HANOW, ALARM, ALERT, ARM, MASK, and TARo. ALARM and ALERT both are location-based routing protocols. Also, they don't use the real node identity which provides in combination with location-based routing increases the privacy and anonymity aspects of the protocols. Only ALARM, MASK and TARo can authenticate origin nodes, thus reducing attack vectors such as identity spoofing and enumeration. The encryption method being used by each protocol has its pros and cons, however ALARM and TARo can be considered less prone to simple attack vectors such as key sniffing, key sharing, and key sharing

VI. CONCLUSIONS AND FUTURE WORK

This paper has presented the anonymous routing protocols. Some protocols provide more security features than the others, such as ALRAM, TARo, and ALERT. The performance of different anonymous routing protocols varies, depending on

the cryptography used and security features provided. In addition, that the security measures affect negatively the performance of the protocols by adding more delays and consuming more of node power [16].

For future work, some areas of the research need more exploration, like measuring of the power consumed by different crypto algorithms, and threat model evaluation of the attacks on the algorithm themselves. Also, simulating the different anonymous routing protocols would help in accurate measuring the delay induced by the algorithms and the security features effects on performance.

REFERENCES

[1] Xiaoyan Hong, Jiejun Kongy, and Mario Gerlay, Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks, Computer sience department, Universty of Aplamba and Aoclahoma. Wireless Communications and Mobile Computing, Wiley, Volume 6, Issue 3, 2006

[2] Jun Liu, Xiaoyan Hong, Jiejun Kong, Qunwei Zheng , Ning Hu , Phillip G. Bradford "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks", IEEE Military Communications conference, 2006

[3] Sk. Md. Mizanur Rahman 1, Atsuo Inomata, Takeshi Okamoto 2, Masahiro Mambo 3 and Eiji Okamoto "Anonymous Secure Communication in Wireless Mobile Ad-hoc Networks", 1st international conference on Ubiquitous convergence technology, Pages 140-149, 2006

[4] Liu Yang Sichuan University, China, Markus Jakobsson, Indiana University Bloomington , USA, Susanne Wetzel, Stevens Institute of Technology, USA."Discount Anonymous On Demand Routing for Mobile Ad hoc Networks". 2006 Securecomm and Workshops, 2006

[5] Yanchao Zhang, Student Member, IEEE , Wei Liu, Wenjing Lou, Member, IEEE,and Yuguang Fang, Senior Member, IEEE "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks.", EEE Transactions on Wireless Communications (Volume: 5 , Issue: 9), 2006

[6] Jiefeng (Terence) Chen National ICT Australia, Australia, and Roksana Boreli, National ICT Australia, Australia, and Vijay Sivaraman School of Electrical Engineering, University of New South Wales,, Australia "TARo: Trusted Anonymous Routing for MANETs", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010

[7] K.U.Leuven, Department Electrical Engineering-ESAT, SCD/COSIC Kasteelpark Arenberg 10, B-3001 Leuven, Belgium "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks", 20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06), 2006

[8] Snehlata Handrale, Prof. S. K. Pathan, " An Overview of Anonymous Routing ALERT Protocol", Department of Computer Engineering,Universaty of Pune, Pune , India, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014

[9] Anupriya Augustine, Jubin Sebastian E, "A Study of Efficient Anonymous Routing Protocols n MANET ", Department of Electronics and Communication Vimal Jyothi Engineering College, Kannur, International Journal of Computer Applications (0975 – 8887), 2014

[10] Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" School of Information and Computer Science, UCLA, IEEE Transactions on Mobile Computing, Volume: 10, Issue: 9, 2011

[11] Kong, J., & Hong, X. ANODR: anonymous on demand routing with untraceable routes for mobile ad-hoc networks, Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing – MobiHoc, 2003

[12] Maity, S., & Hansdah, R. C. Certificate-Less On-Demand Public Key Management (CLPKM) for Self-organized MANETs. Information Systems Security Lecture Notes in Computer Science, 277-293, 2012

[13] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-hoc Networks," Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, 2005

[14] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology," Tech. Rep., February 2008.

[15] Haseeb Zafar1,2, Nancy Alhamahmy1, David Harle1 and Ivan Andonovic, Survey of Reactive and Hybrid Routing Protocols for Mobile Ad Hoc Networks, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 20131

[16] Tianbo Lu, Hao Chen, Lingling Zhao, Yang Li, Anonymous Routing Protocols for Mobile Ad-Hoc Networks (2016), , International Journal of Security and Its Applications Vol. 10, No. 4