Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

An Anonymous Secure Routing Using OLSR Protocol

Osiers Gyamfuah Grace
Department of Computer Science and Engineering, All Nations University College, Ghana
Email: amagrocar@gmail.com
Dr. John Rajan
Department of Computer Science and Engineering, All Nations University College, Ghana
Email: rajan.john@allnationsuniversity.org

ABSTRACT

Security and privacy concerns are major issues to be considered in Mobile Ad hoc Networking (MANET). Several routing protocols have been proposed to achieve both routing and data packets security. In order to achieve privacy, the anonymous routing concept has been introduced and few protocols have been proposed for use in this area. In this paper, global position system (GPS) device is used to obtain the current location of nodes and with the help of a cryptographic algorithm incorporated into the existing Optimized Link State Routing protocol (OLSR), it is expected that security services such as authentication, data integrity, privacy and confidentiality will be provided. This work proposes to protect the network against active attacks such as impersonation and modification.

KEYWORDS: **Anonymous Routing, AODV, Cryptography, OLSR, MANETs.**

Date of Submission: November 13, 2012 Date of Acceptance: January 13, 2013

1. INTRODUCTION

Over the last two decades, Mobile ad hoc networking has caught the attention of several researchers. MANETs has the ability to establish communication structure on-the-fly for emergent and time-critical situations such as the battlefield or military. It is desired that mobile nodes communicate with each other in a secure manner; however, the presence of adversaries as well as the flexible nature of MANETs hinders this goal. A secured MANET environment should be able to provide all or some of these basic security requirements: confidentiality, integrity, authentication, non-repudiation and availability. The traditional routing protocols such as AODV [1], DSDV [2], and OLSR [3], that were initially proposed and designed for MANETs and standardized by the IETF do not explicitly protect the network against attacks and hence do not secure the network. In view of this, several secure routing protocols have been proposed and designed. One area that is currently receiving much attention from the research community in the provisioning of security is anonymous communication.

Anonymity is provided various forms such as sender anonymity, recipient anonymity, route anonymity and relationship anonymity among others. Anonymity is the state of being not identifiable within a set of subjects (i.e. the anonymity set) [4]. Sender anonymity is achieved when a given message is not linkable or traceable to any sender and that to a particular sender, no message is linkable. Similarly, recipient anonymity ensures that a particular message is not tied to any recipient and that to a particular recipient, no message is linkable. Relationship anonymity makes it almost (or completely) impossible to trace two communicating parties.

In certain privacy-sensitive MANET environments like the military or battlefield, communication anonymity becomes the most attractive means of ensuring overall security. This is because, in such environments, it would be preferred that the identity as well as the movement of parties involved in communication be hidden and untraceable. For instance, in a battle field, it is not enough if the basic security requirements are met, leaving the identities and location information of parties involved in the communications exposed to adversaries. In such a situation, adversaries may obtain important information about the location or movement patterns of communication parties, which can be used to locate and launch attacks against them later. To this end, certain protocols have been proposed and designed to achieve anonymity in various forms. Some protocols proposed include the Anonymous Routing Protocol [5], On-demand Lightweight Anonymous Routing [6], Hierarchical Anonymous Routing [7], MASK [8], and Secure Distributed Anonymous Routing Protocol [9].

In this work, the use of MAC addresses of communicating devices is discouraged. This is because, when adversaries get access to that information, then the security and anonymity of those devices will be questionable. The dynamism of the topology of nodes in mobile ad hoc networks implies that their location addresses will keep changing. Hence, instead of using IP and MAC addresses, a GPS device could be used to obtain the coordinates (i.e. location) of mobile nodes.

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

This location information can then be securely exchanged between nodes in the network. Once a link has been securely and anonymously established between parties, a shared secret key can be used to encrypt communication to achieve both security and privacy. The contribution of this work is in two folds:

i. Providing sender, recipient and route anonymity.
ii. Incorporate affordable encryption scheme into the existing optimized link state routing protocol.

The rest of the paper is organized as follows: related work is discussed in section II. Section III presents a brief overview of the OLSR protocol and its inherent security issues. Section IV focuses on securing and anonymizing the OLSR protocol. In section V, the performance of the secure OLSR is analyzed based on extensive simulation. The paper concludes in section VI with a summary and proposed future work.

2. RELATED WORK

Secure communication in the Mobile Ad hoc Networks is of a major concern to researchers. Several secure routing protocols; both proactive and reactive have been proposed. This section presents a brief overview of few of these existing protocols.

In 2002, Yih-Chun Hu and Adrian Perrig proposed ARIADNE. ARIADNE protects the network against malicious nodes that tampers with uncompromised routes and Denial of Service attacks. This protocol employs symmetric cryptography to protect and authenticate routes [10]. Unlike the anonymous routing, ARIADNE makes use of both sender and receiver explicitly. Similar to ARIADNE protocol are SEAD[11], SAODV[12], ARAN[13], SRP[14], among others, which all employ various hop-by-hop encryption schemes to authenticate nodes and routes in the network, paying no attention to anonymity. Encryption schemes are able to protect the network against eavesdropping and masquerading attacks [cryptography book] thereby ensuring data integrity and node (sender and/or recipient) authentication. However, issues concerning location disclosure and traffic analysis attacks have not been well addressed by existing cryptographic approaches.

In an attempt to provide solution to the location disclosure and traffic analysis attacks, anonymous routing protocols have been adopted. Anonymous protocols could be designed to function as on-demand or proactive. Haiying Shen, et al [15] categorizes the existing anonymous routing protocols as those based on hop-by-hop encryption and those based on redundant traffic routing.

ASPRAKE [16] provides anonymity from all intermediate nodes. It uses ring signature based on ECC to achieve an authenticated key agreement. ASPRAKE achieves end-to-end anonymity, to the neglect of sender and receiver anonymity. Jun Pan, et al proposed MASR [17], an anonymous protocol which achieves identity anonymity, location anonymity and route anonymity. MASR masks both the source and destination addresses, contrary to ASPRAKE and also provides a symmetric trapdoor.

In [5] Bu Zhu, et al, proposed the anonymous secure routing (ASR) that spices the anonymity world with strong location privacy, protecting the network against several passive and active attacks.ASR exploits the benefits of shared secrets between two successive nodes to achieve security and privacy, close to the use of route pseudonym in ANODR[18]. The shared secrets are used to authenticate successive intermediate nodes before the data is transmitted. The hop-by-hop authentication may introduce additional cost and burden on the nodes since no central authority is employed to do that. Also, the use of public key in such a manner makes it easy for attackers to run a trace on the source and destination nodes. Similar to ANODR, during message transfer, MASK [8], encrypts and decrypts data packets at each hop using the shared secret of each pair of adjacent nodes, generated during the anonymous neighborhood authentication process. MASK is unable to hide the identity of destination nodes.

In [7], Jun Liu, et al proposed HANOR, which takes hierarchical MANET structures into design decision and provides two levels of anonymity namely intra-group and inter-group anonymity. Unlike ALERT, HANOR is not able to achieve individual sender or recipient's anonymity. SDAR [9] protocol allows intermediate nodes that are trustworthy to participate in the path construction protocol. SDAR uses a community key management system making it more secure. However, identities of all the forwarders and their shared secrets are known to the destination, violating the sender anonymity concept.

In [21], the authors proposed a proactive link state protocol, capitalizing on the periodic update feature of proactive protocols. ALARM periodically broadcasts information on nodes' location to all authenticated nodes within the network to equip each node with enough information to build a topology map which can be used for anonymous route discovery and data transmission. Authors in [15] argues that the map construction can lead to a situation where location information of destination nodes are leaked, compromising the route anonymity.

An example anonymous routing protocol that does not use hop-by-hop encryption and decryption is MAPCP [19]. It uses broadcasts with probabilistic-based flooding control to create multiple anonymous paths among communication parties. This protocol achieves source and destination anonymity to the neglect of location or route anonymity. The elimination of the hop-by-hop encryption obviously reduces computational complexity and seems to conserve power.

In this work, it is assumed that mobile devices involved in the communication are all equipped with GPS devices that are able to provide coordinates or physical location of each device (or node). These coordinates are then used in routing instead of using MAC addresses; serving as pseudonyms. A hop-by-hop encryption mechanism is used to provide data security and integrity. Unlike some of the reviewed literature, this works

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

proposes to achieve sender, recipient and route anonymity and minimize the encryption overhead as much as possible by the use of shared secrets.

3. OLSR PROTOCOL AND SECURITY

This work focuses on enhancing the security of the OLSR routing protocol as well as making it anonymous protocol. A brief overview of the existing OLSR protocol and security issues addressed by other researcher are studied and analyzed.

3.1. OLSR Routing Protocol

OLSR, a proactive routing protocol designed for communication in ad hoc networks, inherits the stability of link state algorithms and has the advantage of having routes immediately available when needed due to its proactive nature. OLSR is an optimization over the classical link state protocol. It exchanges topology information with other nodes of the network regularly. In OLSR, unlike other proactive routing protocols, each node selects a set of its neighbor nodes as multipoint relays (MPR). Only these MPRs are responsible for forwarding control traffic, intended for diffusion into the entire network. The MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required [3].

In OLSR, two different types of control traffic (messages) are exchanged. These are the HELLO and TC (topology control) messages. HELLO messages are transmitted periodically by a node and contain three lists: list of neighbors from which control traffic has been heard, list of neighbor nodes with which bidirectional communication has been established, and list of neighbor nodes that have been selected to act as MPR for the originator of the HELLO message. HELLO messages are only exchanged between neighbor nodes and are not forwarded further. OLSR may optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission. The core functionalities of the OLSR protocol include Packet Format and Forwarding, Link Sensing, Neighbor detection, MPR Selection and MPR Signaling, Topology Control Message Diffusion, Route Calculation [3].

3.2 OLSR Core Functionalities

3.2.1. Neighbor Discovery

In this functionality, each node discovers other nodes which fall within its communication range directly (One - hop neighbors). A Node at this stage finds out nodes or routers with which bidirectional communication can be established. Each node sends HELLO messages, indicating the addresses of all the nodes it has recently communicated with as well as the status of the link (heard, verified bi-directional). With the help of periodic HELLO, a node B can get to know the neighbors of its neighbors (two – hop neighbor) [18].

3.2.2. Link Sensing

Link Sensing is accomplished by sending HELLO messages over the interfaces through which connectivity is checked periodically [3][20]. A separate HELLO message is generated for each interface. A local link set which describes links between local and remote interfaces are the results of the link sensing.

3.2.3. MPR Selection and MPR Signaling

The objective of MPR selection is for a node to select a subset of its neighbors such that a broadcast message, retransmitted by these selected neighbors, will be received by all 2-hop neighbors [20]. The MPR set of a node is computed such that for each interface, it satisfies this condition. Each node maintains an MPR selector set, describing the set of nodes which have selected it as an MPR. The information required to perform this calculation is acquired through the periodic exchange of HELLO messages.

3.3. Security Issues in OLSR

The MANETs environment presents quite a number of security issues that needs to be considered and addressed. Some of these issues are related to the physical nature of the wireless links in the networks. Others are security problems that are also present in the wired network**.**

As a proactive routing protocol, OLSR periodically disseminates it topological information, which if used in an unprotected wireless network, implies that network topology is revealed to anyone who listens to OLSR control messages, making it difficult to achieve topology (sender, recipient and route) anonymity.

Again, OLSR operates under the assumptions that each router can maintain a topology map that reflects the effective network topology. It is assumed that all nodes in the network have enough identical network topology maps. If any of these assumptions no longer holds, nodes may either not be able to obtain topological maps of the network or get topological maps that does not reflect the true state of the network topology. This may also result in a situation where multiple routers obtain inconsistent topological maps [20].

The OLSR, like AODV, has been designed without any security measures put in place. It provides no mechanism to validate the authenticity of either hello messages or TC messages. Nodes trust apriori every message they receive and may update their neighbor set with fake information. This makes the OLSR susceptible to various attacks from intruders who may take advantage of this lack of verification to launch attacks. Some of the known attacks and vulnerabilities of the OLSR include identity spoofing, link spoofing, failure in relaying TC messages, wormhole attacks [22].

In OLSR, each node is able to infuse topological information into the network with the help of either HELLO messages or TC messages. If a malicious node injects invalid control traffic, the integrity of the network will be jeopardized. OLSR is highly susceptible to *Denial of Service* (DoS) attacks. A malicious node could false OLSR packets containing false information in large amounts. Processing of such huge data could put unnecessary stress on all resources on the receiving

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

nodes, hence, making them unable to handle any other tasks. This may lead to the crash of the OLSR service, making the node unavailable eventually

The OLSR protocol is vulnerable to Identity and link spoofing. In Identity spoofing, a malicious node sends control messages pretending to be another node, violating the authentication service. The Link spoofing attack involves the sending of control messages containing an incorrect set of neighbors. This may result in routing loops and conflicting routes in the network. If a malicious node deliberately sends an incomplete set of neighbors, it may cause a breakdown in connectivity with the rest of the network, leading to dead ends.

Another security vulnerability of the OLSR protocol is wormhole attack. This attack involves the collusion of two malicious (A and B) or attacker nodes with the help of a link. Traffic received by **A** is forwarded through the wormhole link to **B**, for later rebroadcast by B. The reverse is true. In OLSR, an attacker can use an intruder node residing in the region or zone of both A and B to send HELLO messages from A to B and vice versa.

In addition to the aforementioned vulnerabilities, OLSR protocol is vulnerable to attacks such as sequence number attacks [20], message timing attacks [20], among several others.

4. SECURING OLSR

This work inherits the basic assumptions of the ALARM protocol [19]. It is assumed that nodes employed here are all GPS-enabled, readily providing location information. Attacks that are launched based on providing fake, non-existent addresses can be thwarted if there exists position information on each node. If such information exists, then nodes can compare this geographical data to the received routing data (i.e. the neighbor and link set). If contradictory information is found, the false routing message is detected and discarded.

In this work, it is also assumed that all nodes join the network at the same time and are equipped with RSA public and private key pairs. Nodes that belong to an MPR selector set make their public keys known to the MPR by a unicast message to the MPR in a format like: Msg = {hello||Loc_Info||Puk_{si}

These nodes s_1, s_2….s_n receive a message which now contains the public key of the MPR encrypted with their public keys respectively. The message received from the MPR is of the form: $Msg_{(mpr)}$= [Puk s_1{helloReply||Loc_Info||$Puk_{(mpr)}$}] with a digital signature [eg. Hash functions like MD5, SHA] computed over these fields. On receiving this message, both the MPR and the corresponding nodes can authenticate message received from each other. When a node receives a new message, it checks whether the message is not duplicated. If not, it then verifies the signature by re-computing the hash value and compares it to the received one. If they match, then the integrity, confidentiality as well as the authentication of the message is assured. After this, the MPR can encrypt a shared secret, S, using the public key of the corresponding node with which it wants to communicate. This secret key is then used for communication between these two nodes. It is important to note that even the GPS-enabled nodes can still choose to fabricate incorrect location information in order to launch Sybil attacks.

This can be summarized as follows:

- Nodes s_1, s_2….s_n send their public key information to the MPR node in the form:
  Msg = {hello||Loc_Info||Puk_{si}}.
- MPR node replies by including its public key in the message and encypting with node s_1, s_2….s_n public key respectively:

$Msg_{(mpr)}$=[$Puks_1${helloReply||Loc_Info||$Puk_{(mpr)}$}]

- Node receives a new message and check whether it is a duplicate or not. If it is, discard message.
- Else, re-compute hash value and compare it to received one. If they match, then signature is valid hence message can be trusted.
- Then, $Msg_{(mpr)}$ = [puk_{s1}{s}]
- S_1 and MPR now communicates using S.

Both single malicious node and multiple malicious nodes are introduced into the network within which the secure OLSR operates. The OLSR performance is compared with the performance of the AODV protocol in similar situation. The results obtained are briefly discussed and analyzed in the next section.

5. PERFORMANCE ANALYSIS

5.1 Simulation Parameters

Simulation Parameters

- ✓ Simulation is done using NS-2.34 network simulator with MANET extensions.
- ✓ IEEE 802.11 is used as the MAC layer protocol.
- ✓ The radio propagation model used is the two-ray ground model.
- ✓ The traffic pattern is CBR (Constant Bit Rate) with a packet length of 512 bytes.
- ✓ The mobility model used is the Random Waypoint Model
- ✓ The simulation time is 100 seconds for AODV, DSR and 50seconds for OLSR
- ✓ The number of nodes used varied in 10's starting from 10 to 50.

5.2 Performance Metrics

The proposed secured OLSR routing protocol is evaluated based on the following metrics:

- Packet Delivery ratio
- End-to end delay and
- Throughput.

End to End Delay indicates the time lapse between the source nodes and destination nodes in the network. *Throughput,* In computer technology, is the amount of work that a computer can do in a given time period. T**hroughput** can be said to be the average rate of successful message delivery over a communication channel and its normally measured in bits per second (bit/s or bps). Packet delivery ratio indicates the ratio of

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

packets delivered to the total packets that were transmitted.

5.3 Simulation Results.

Throughput is the one of the main measuring parameters of this work. It shows the effectiveness of an implementation. From the Fig1, it is evident that AODV and DSR have high throughputs under normal condition.

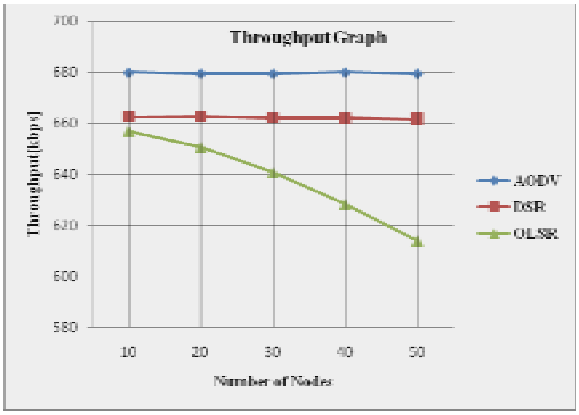

Fig1- Throughput graph of AODV, DSR, and OLSR

However, the graph shows that throughput of the OLSR protocol decreases as number of nodes used in the simulation increases. This could be attributed to packet loss experienced by the protocol. OLSR is actually designed for dense networks. Considering the throughput graph of the OLSR, it is expected that the delay will increase. Interestingly, this is not the case. As the number of nodes increases, the delay decreases to a point and then start rising again as indicated in Fig2 below.

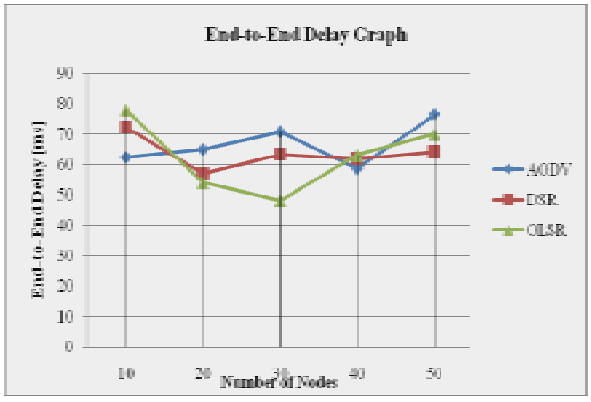

Fig2. End-to-end delay of AODV, DSR, and OLSR

Malicious nodes ranging from 1 to 5 were introduced in both the AODV and OLSR routing protocols and their performance under such condition were observed. From the graph in Fig3, it is seen that both AODV and OLSR have similar end-to-end delay time when under malicious attacks. The malicious nodes introduced are within 0 and 6. When the malicious nodes equal 3, the delay was almost equal.

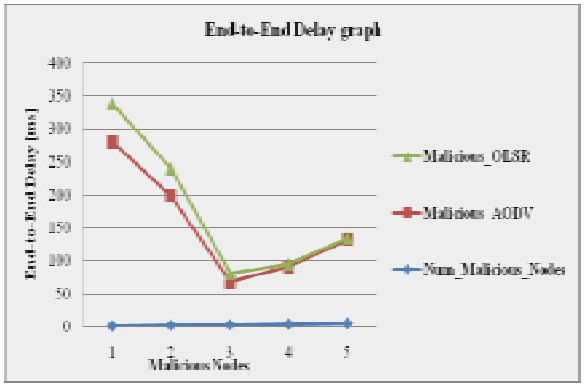

Fig3. End-to-end delay graph of OLSR and AODV under malicious attack.

Measuring the throughput of both OLSR and AODV yields an interesting result. From Fig4 below, throughput of OLSR starts at a very high point compared to the AODV and finally comes to a point as low as the AODV. This indicates that the secure OLSR is more robust than the AODV in the presence of adversaries.

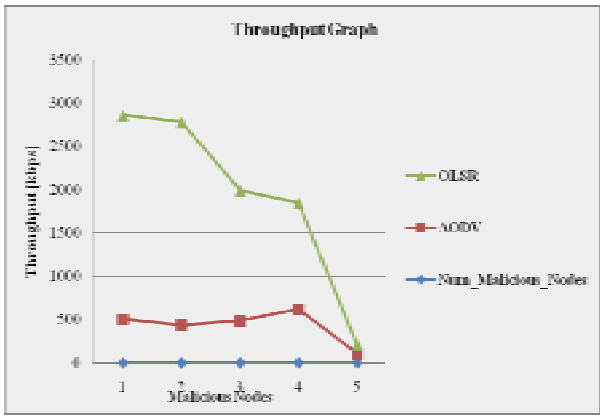

Fig4. Throughput graph of OLSR and AODV under malicious attack

The robustness of the OLSR becomes much evident when the protocol is employed in denser network environments. In a dense environment that is under adversarial attack, Fig5 indicates that the protocol's throughput is still desirable, though the delay also increased. As part of the future work, the delay would be reduced.

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

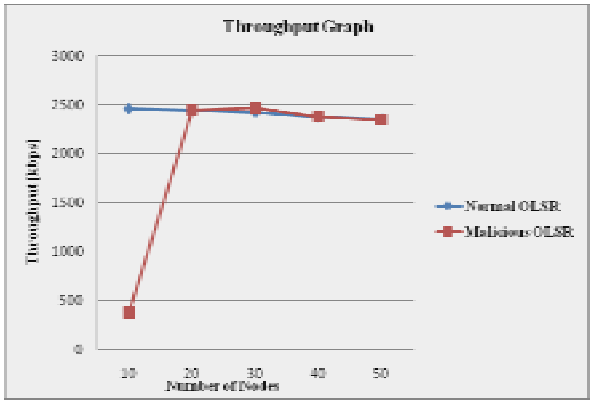

Fig5. Throughput graph of normal OLSR and OLSR under malicious attack

6. CONCLUSION AND FUTURE WORK

It is a desirable property of MANET to ensure that communication within and without the network is secure. This however is hampered by adversaries who may want to modify, delete or simply eavesdrop on a communication between some parties. In this work, the security of the existing OLSR routing protocol has been enhanced with the help of cryptographic algorithm, providing sender, recipient and route anonymity. Security services such as authentication, data integrity and confidentiality were provided. The use of cryptographic primitives seems to increase the overhead. However, this will be reduced after connection has been established, since symmetric shared secrets key will be used. Extensive simulation was done to analyze the performance of the secure OLSR.

This work limits the number of nodes used to 50 and malicious nodes were only introduced in AODV and OLSR routing protocol. In future, the number of nodes used will be increased and also malicious nodes will be introduced in DSR routing protocol. Also, the issue of sybil attacks will be considered and dealt with.

REFERENCES

[1]. C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications*, 1999, pp. 90–100.

[2]. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *ACM SIGCOMM '94*, 1994.

[3]. P. Jacquet, P. Muhlethaler, and A. Qayyum, "Optimized Link State Routing Protocol," *RFC 3626*, Oct. 2003.

[4]. Andreas Pfitzmann and Marit Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – *A Consolidated Proposal for Terminology"*, (Version v0.25 Dec. 6, 2005).

[5]. B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," in *29th IEEE International Conference on Local Computer Networks (LCN'04)*, 2004, pp. 102–108.

[6]. Qin, Yang, Dijiang Huang, and Vinayak Kandiah, "OLAR: On-demand lightweight anonymous routing in MANETs." *The Fourth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, 2008.

[7]. Liu, J., Hong, X., Kong, J., Zheng, Q., Hu, N., & Bradford, P. G. (2006, October). A hierarchical anonymous routing scheme for mobile ad-hoc networks. In *Military Communications Conference, 2006. MILCOM 2006. IEEE*(pp. 1-7). IEEE

[8]. Yanchao Zhang Wei Liu ; Wenjing Lou ; Yuguang Fang , "MASK: anonymous on-demand routing in mobile ad hoc networks ", *Wireless Communications, IEEE Transactions, Volume: 5* , Issue: 9 , September 2006, Page(s): 2376 – 2385

[9]. Boukerche, A., El-Khatib, K., Xu, L., & Korba, L, "SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks", In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on* (pp. 618-624). IEEE.

[10]. Y. Hu, A. Perrig, and D. B. Johonson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), Proc. ACM MobiCom '02*, Sept. 23–26, 2002.

[11]. Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Proc. IEEE Mobile Computing Systems and Applications*, 2002, pp. 3–13

[12]. B. Dahill *et al.*, "ARAN: A secure Routing Protocol for Ad HOC Networks," *UMASS Tech Report*, 2002 pp. 2–32.

[13]. Zapata, Manel Guerrero. "Secure ad hoc on-demand distance vector routing."*ACM SIGMOBILE Mobile Computing and Communications Review* 6.3 (2002): 106-107. M.

[14]. Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad hoc Networks", *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, January 27-31, 2002

[15]. Zhao, Lianyu, and Haiying Shen. "ALERT: An anonymous location-based efficient routing protocol in manets." *Parallel Processing (ICPP), 2011 International Conference on*. IEEE, 2011.

[16]. X. Lin, R. Lu, H. Zhu, P. -H. Ho, X. Shen, and Z. Cao, "ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for

Int. J. Advanced Networking and Applications
Volume: 04 Issue: 04 Pages: 1645-1651 (2013) ISSN : 0975-02

wireless ad hoc networks," in *Proceedings of the IEEE International Conference on Communications (ICC '07)*, 2007, pp. 1247–1253.

[17]. Pan, Jun, and Jianhua Li. "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks." *Management and Service Science, 2009. MASS'09. International Conference on*. IEEE, 2009.

[18]. J. Kong and X. Hong. ANODR: ANonymous on demand routing with untraceable routes for mobile ad-hoc networks. In *Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03)*, 2003, pages 291–302,

[19]. Chao-Chin Chou, David S. L. Wei, C.-C. Jay Kuo, and Kshirasagar Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-hoc Networks", *IEEE Journal On Selected Areas In Communications, Vol. 25*, No. 1, January 2007, pp 192-203

[20]. Clausen, Thomas, and Ulrich Herberg. "Vulnerability analysis of the optimized link state routing protocol version 2 (OLSRv2)." *Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on*. IEEE, 2010.

[21]. El Defrawy, Karim, and Gene Tsudik. "ALARM: Anonymous location-aided routing in suspicious MANETs." *Mobile Computing, IEEE Transactions on* 10.9 (2011): 1345-1358.

[22]. Clausen, Daniele Raffo Cedric Adjih Thomas, and Paul Mühlethaler. "OLSR with GPS Information".

Authors Biography

Osei Grace Gyamfuah received her M.Tech degree in Software Engineering in 2009 from SRM University, India. She is pursuing her Ph.D in the Computer Science and Engineering Department at SRM University. Her research Interests include wireless networks, security and routing in Mobile Adhoc networks. At present she is working as a Lecturer at All Nations University College, Koforidua, Ghana

Dr. Rajan John obtained his Ph.D. from Karunya University. He is specialized on automated and unified data mining using intelligent agents. His research areas include data warehousing and mining, software agents and cognitive systems. He is working as Assistant Dean, All Nations University College, Koforidua, Ghana, West Africa.