*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VI (Sep-Oct. 2014), PP 47-54*
*www.iosrjournals.org*

# An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location

Jyothis B. Kallada, Renjith George
*Dept. of CSE Ilahia College of Engineering and Technology, Kerala, India*
*Assistant Professor Dept. of CSE Ilahia College of Engineering and Technology, Kerala, India*

***Abstract:*** *The protocols and cryptographic techniques used in MANET are intended to provide complete security to the data transmitted with low cost. In hostile environments, as a part of providing security to data; the source, destination and route of the data need to be anonymous. Prior works do not provide complete anonymity protection along with security, reduced network overhead and cost, sever side security and efficient utilization of resources. So "An Efficient Secure Anonymous Communication Protocol in MANET based on Destination's Location is proposed". This paper "An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location" uses a technique called one-hop-distance; one-hop-distance along with public key encryption technique provides security of data and anonymity of route and destination. To provide source anonymity, this paper presents the concept of a proxy node. The technique one hop distance presents in this paper can also prevent different types of attacks such as intersection attack, black hole attack etc…, and can reduce the network overhead and cost of data transmission. Their by the resources in MANET can be efficiently utilized to the maximum.*

***Key words:*** *MANET, anonymity, hop, GPSR, Hostile Environment.*

## I. Introduction

MANET is Mobile Ad Hoc Network in which, a group of mobile devices can communicate with each other without using any fixed network infrastructure by dynamically forming a network and it is self configuring. Since the nodes in the network are mobile, wired connection makes some difficulty or is not possible at all. In MANET, the nodes which are not in range can communicate with each other using the intermediate nodes which are in range by constructing a path. Due to the exploitation in the field of Mobile Ad Hoc Networks and because of its features of self organizing and independent infrastructure, it is used in a large number of wireless applications in the areas such as military, education, entertainment etc…

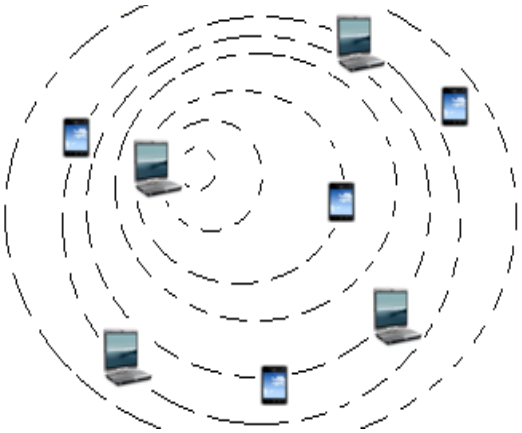

Fig 1: Mobile Ad Hoc Network

Anonymous protocols used in MANETs are intended to provide anonymity protection to source, destination and route. Source and destination anonymity aims to protect the real location and identity of source and destination from inside or outside attackers. Route anonymity aims to hide the data flow path between source and destination. Many works fails to provide the all above mentioned anonymity protection with strong security. For example ALARM cannot provide location anonymity destination and route anonymity [3], Ariadne mainly focusing on route anonymity [4] and AO2P do not provide route anonymity [6].

Many routing protocols uses geographic routing [2], [11], [12], in which, routing decision is based on geographic superiority among neighboring nodes. Prior works uses symmetric cryptographic primitives [4], and hop-by-hop encryption [2], [3], for route anonymity, that exacerbates high cost. The high cost over burn

resource constraint problem in MANET. Thus the limited resource availability may badly affects educational approaches, military operations etc. Security and integrity of data is an important concern in military operations. So MANET employed in a battlefield should be highly efficient and secure with minimum cost and network overhead.

In order to meet the requirements of high anonymity protection (to source, destination and route), security and reduced network overhead with minimum cost for data transmission, "An Efficient Secure Anonymous Communication Protocol in MANET based on Destination Location" is Proposed. This protocol uses a technique called one-hop-distance in which, after receiving the data from source node through intermediate nodes, the destination node forwards the data to another node in its range and this node again sends the data back to the destination node. Their by destination anonymity can be provided and also black hole attack can be prevented. Public key encryption along with hierarchical zone partitioning can be used to provide route anonymity. This protocol uses a proxy node strategy to hide the data sender. The one-hop-distance technique along with public key encryption used in this paper can send the data with minimal network overhead, reduced cost and high security.

## II. Related Works

Routing protocols in MANETs are grouped into two: *Reactive* or *on demand* [17], [8], [18], [2] and *Proactive* [3] routing protocols. Reactive routing protocols use route discovery to identify a route. Proactive routing protocols are of two type: *link- state* and *distance vector protocols.*

In MANETs, routing is mainly based on GPSR algorithms [10], [11], in which data is transmitted from source to destination based on geographic superiority of nodes. A node that sends data to another node mainly focuses the position and distance of destination node from that node. So an attacker on getting the position of destination or source can get the route by continuous monitoring of the network.

In order to provide location privacy, an idea of disseminating user identity with its location [2] based on GPSR is used. But, this cannot provide route anonymity. Because in GPSR algorithms [2], [10], [11], data routing is based on shortest distance between the nodes. So adversary in long transmission session can easily identify the route by continuous monitoring of network. If route is identified then source and destination can be easily identified.

In hop-by-hop encryption [8], [2], [6], each hop that receives the packet, decrypts it and send to next hop. This is to prevent adversaries from tapering or analyzing the data. The number of encryption and decryption increases with the number of nodes in the path from source to destination increases. This happens when source and destination are in long distance apart from each other, which requires large amount of energy and generates high cost. This leads to limit the efficient utilization of resources in MANET and exacerbates resource constraint problem.

In hostile environment privacy-preserving secure communication is very important. ALARM [3] offers strong security and privacy in suspicious MANETs. Link state protocols such as OLSR [12], can provide stronger security using techniques [14], [15] and [13], so origin authentication and integrity of LS updates can be done easily. But ALARM do not provides location anonymity of destination, since each node broadcast its location information to its neighbors, this authenticated neighbor can build a map, their by route anonymity can be compromised.

In AO2P [6] a node en route data selects another node on the basis of reducing the largest distance from the destination. AO2P uses pseudonym to protect nodes real identities. But it does not provide destination anonymity. Advanced AO2P avoid this problem by finding a node in the path from source to destination, which is further from source than destination. This node replaces exact destination with this position for distance calculation.

In order to authenticate the nodes en route, Ariadne [4], along with TESLA [16], uses broadcasting. Broadcasting can cause traffic problems, and may results in network overhead. Ariadne uses symmetric key cryptography for authentication, but SEAD [9] uses low-cost one-way hash functions. But all of these hop-by-hop encryption method results in high cost because of the use of hop-by-hop public-key cryptography or complex symmetric key cryptography.

Topology based routing is performed in ANDOR [8]. It uses hop-by-hop encryption in reactive routing protocol. Aad[17] adds to ANDOR onion routing, multicast, and packet coding capabilities. ANDOR provides source, destination and route anonymity, but it do not provide location anonymity of source and destination. Trapdoor

boomerang onion routing is used in ANDOR. The onion construction used in ANDOR for route discovery and return route generate high cost. To avoid this problem Discount-ANDOR[18] is proposed.

Redundant traffic [3], [17], includes flooding, multicast and local broadcasting, this to obscure attackers. In MAPCP [5], every node en route performs probabilistic broadcasting, in which each node selects its neighbors with a certain probability to forward the message. MAPCP uses redundant traffic and it acts as a

middleware between network and application layer. MAPCP uses geographic routing and provides identity anonymity of source and destination along with route anonymity. But MAPCP do not focus on location anonymity of source and destination.

ALERT [1], uses k-Anonymity model [7]. In ALERT, after calculating destination zone, data is broadcasted to k nodes in that zone. Their by ALERT provides destination anonymity, but broadcasting can cause network overhead. ZAP [19], uses redundant traffic, which impose high cost on redundant operations. Geographic routing is performed in ZAP, in ZAP destination anonymity is provided by local broadcast to destination zone, but ZAP do not provide route anonymity.

## III. Proposed System

The proposed system is "An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location", which can be used in different node movement pattern such as random way point model, and group mobility model.

In geographic routing, data is routed from source to destination through the shortest path. In the proposed system hierarchical partitioning along with geographical routing is used for routing. The proposed system uses a technique called one-hop-distance and public key encryption to provide anonymity protection and makes the system resilient to black hole and intersection attacks. Otherwise an attacker performing intersection attack can easily reveal the position of destination. The hierarchical zone partitioning is used to discover the path from source to destination. The public key encryption technique with hierarchical zone partitioning is used to provide route anonymity and the proxy node concept provides anonymity protection to source.

The technique one hop distance used here can reduce the network overhead and the cost of data transmission, their by it increases the overall performance of the system. By eavesdropping, the attacker can understand the protocols used in the network for routing, and also get the position of nodes in the network; also the attacker can capture the data on fly. By performing denial of service attack on vulnerable node, the attacker can compromise that nodes and can obtain complete details of historical communication. Their by the attacker can perform malicious activities on the network.

The intruder is considered to be battery powered nodes. The symmetric and public / private key decryption requires reasonable amount of time, because the resources of attacker is limited. The encrypted data is secure to a certain degree, if the attacker is not clear about the key.

## IV. Solution Methodology

"An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location", provides complete anonymity protection to source, route and destination with very high security to the data transmitted using public key encryption. It also reduces the network overhead their by the cost of data transmission can be reduced and is resilient against black hole, intersection and timing attacks.

**Pseudonym and Location Server Concept**

The communication is possible only if the communicating parties know the address of each other. In MANETs, the ip address or MAC address is used for communication. An attacker compromising a packet can easily reveal the source and destination by identifying the MAC address. So the concept of pseudonym is proposed. It is a random number used as node identifier instead of MAC address. The SHA-1 algorithm uses a nodes MAC address and current time stamp to avoid pseudonym collision. The time stamp is too short (e.g., nanoseconds), to prevent attacker from computing the pseudonym.

Dynamic pseudonym is used so that, even though an attacker identifies a nodes pseudonym cannot connect to that node. Since the pseudonym dynamically changes, every nodes routing table contains neighbor's pseudonyms with their location. Each node obtains this information from the 'hello' messages with updated position and pseudonym, from its neighbor's.

If a node wants to communicate with other node, it needs the location and the public key of other node. It is assumed that the public key and location of destination is known by other nodes as in AO2P [6]. Secure location service [19], allow a source node knowing the identity of destination node in identifying the public key and location of destination. Each node is associated with a location server and shares a secret key with it. If a node X wants to communicate with a node Y then, X requires the position and location of Y, for that X sign's its request containing Y's identity with its identity and sends this request to its location server using the secret key shared between them. The encrypted response message contains Y's location and public key which is decrypted by X, using the pre-distributed secret key. The public key is used to share a symmetric key $K_s$ between these two nodes for secure communication. Server data is encrypted to provide security.

**Anonymity Protection to Source**

MANET employed in hostile environment such as law, military requires high anonymity protection. The view of source is restricted to only its neighbors. To strengthen the source anonymity protection, a proxy node concept is used. The proxy node is a node in the neighborhood of source node. Here the proxy node sends packet at the same time, when source node is sending the packet. Here "notify and go" mechanism is used.

As [1], in the notify phase, source piggybacks its data transmission notification to its neighbor's with periodical update packet, that it is going to send a packet. The t and $t_0$ are the two random back-off time periods present in the packet. The $t_0$ should be an optimum value to minimize interference, because too many packets send out data at the same time.

Many proxy nodes can send packets at same time, when source is sending the packet, which may cause network overhead. So it is necessary to prevent the flow of packets from the proxy node after the first phase. In order to do this, a valid TTL field is inserted in the packet of original source and the TTL=0 is inserted into the packet of proxy node as in [1]. To differentiate the source packet from proxy nodes packet, source encrypts its TTL field using $K^{RN}_{pub}$ obtained from periodical hello packets of the neighbor's.

**Route Anonymity, One-Hop-Distance and Destination Anonymity**

The route from source to destination needs to be anonymous. In order to provide route anonymity, hierarchical zone partitioning and public key encryption is used.

Here the entire area of network, where MANET disseminated is cosidered to be a rectangle. Each node in the network is configured with the the top-left and bottom right corner of the rectangle, when it joins the system. In hierarchical zone partitioning, whenever source 'S' wants to send data to destination 'D', source S first divides the entire area vertically or horizontally into two halves, so that source and destination are in two separate halves. S then selects a node in other zone as temporary destination TD and forwards data to TD through intermediate relay nodes.

The horizontal and vertical partitionig are performed alternatively. The TD which is the new source, divides the entire area vertically into two halves so that the destination and new S are in two separate zones. Again this S finds a node in other zone as TD and forwards the packets to TD through intermediate relay nodes. These intermediate relay nodes are also called data forwarder. This process is continued untill the destination is reached. The relay node selects a node in the other zone as random forwarder, if that node is the node having shortest

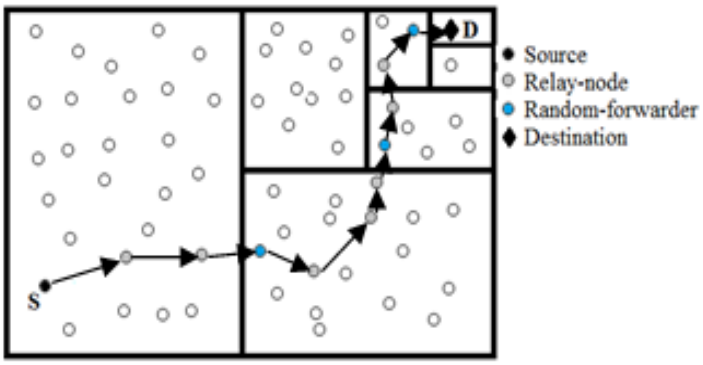


Fig 2: Rounting from zone to zone distance from the relay node.

This crieteria is based on GPSR [2] algorithm.

Here after the first horizontal partition two generated zones are (0,0), (xG,$0.5_{yG}$) and ($0,0.5_{yG}$), (xG,yG). Again the source perform verical partitionig in the zone where destination resides. This process is continued recursively until the destination node is reached.

"An Efficient Secure Anonymous Communication Protocol in MANET based on Destination's Location" provides location and identity anonymity of source, destination and route. The random forwarder RF changes, because RF's are selected randomly in the transmission of each packet. Thus it is difficult for an attacker to identify the statistical pattern of transmission. Here the random forwarder is only aware of the preceeding and suceeding nodes, so source and destination cannot be identified. Therefore the transmitted data cannot link the source and destination.

In this protocol the source to destination route are constantly changing, so it is difficult for an intruder to predict the next hop. The number of nodes participated in routing for a single communication is very large, because route is constantly changing in each communication and the strong public key encryption prevents the attacker from stopping the communication, even if few nodes are compromised.

One-hop-distance along with public key encryption provides anonymity protection to destination and route. The source node with the help of location server determines the route, through which data has to be send from source to destination.

Example 1: A is the source node and D is

the destination node. If node A sends message to node D. The message passes through the intermediate nodes B and C to reach the node D. If E is one of the neighbor of destination node D. Then according to the concept of one-hop-distance, the message after reaching destination D goes to node E and then return backs to D from E. Fig 3, shows the routing path.

The source encrypts data field in the packet with the secret key $K^{A}_{s}$ shared between source A and destination D to produce encrypted data, $[DATA]K_s$. The server add parity bits to the routing field. Then the routing field and data field is encrypted with the public key of node D, this encrypted data can be represented as $X_D$. Then the server add identity of node D to routing field. This field and the encrypted

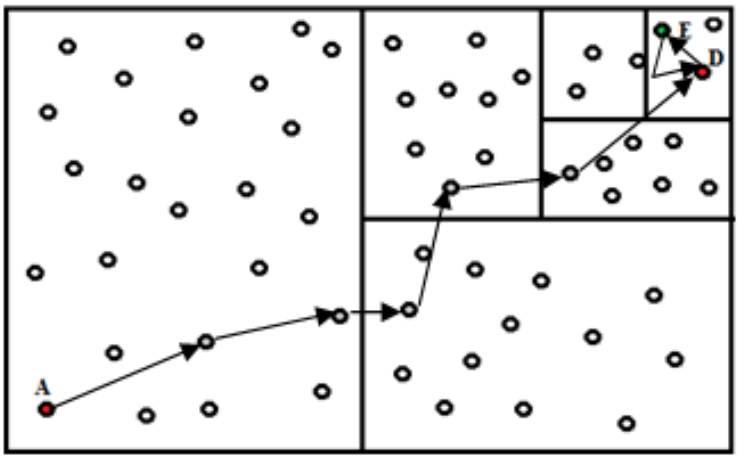


Fig 3: Routing based on One-Hop-Distance

data is again encrypted with the public key of node E. Again identity of node E and encrypted data is encrypted with the public key of node D. This process is continued untill B encrypt the identity of node C and the previously encrypted field with its public key, $K^{B}_{pub}$. This stepwise encryption is shown in figure 4. Here A is the source node, so it do not encrypt the next hop identiy (here it is B's identity) and data field with its public key $K^{A}_{pub}$.

The public key encryption technique used here, strengthen the anonymity protection of route, because even though a packet is compromised, the attacker cannot identify the route to reach the destination, since the routing field is encrypted continuously with public key of different nodes, which require the corresponding private key to decrypt it. The private key of each node is kept secret, which is only known to that node.

The concept of one-hop-distance prevent an attacker, who is monitoring the network from identifying the destination, since after receiving the data, destination forwards data to a neighboring node, their by an attacker focusing on the network, thinks that the destination node is only a normal node that en routes the data. So destination anonymity can be provided. In previous work [1], k-anonymity model is used to provide destination anonymity, which employs broadcasting and results in network overhead and generates high cost.

| Routing Field | Data Field | | Encrypted Data |
|---|---|---|---|
| 0 0 0 0 | $[DATA]K_S$ | $E_K{}^{D}{}_{pub}$ | $X_D$ |
| D | $X_D$ | $E_K{}^{F}{}_{pub}$ | $[X_D]_E$ |
| E | $[X_D]_E$ | $E_K{}^{D}{}_{pub}$ | $[[X_D]_E]_D$ |
| D | $[[X_D]_E]_D$ | $E_K{}^{C}{}_{pub}$ | $[[[X_D]_E]_D]_C$ |
| C | $[[[X_D]_E]_D]_C$ | $E_K{}^{B}{}_{pub}$ | $[[[[X_D]_E]_D]_C]_B$ |

Fig 4: Encryption of Routing Path

The routing performed here is based on hop by hop decryption. Here source A send packet to next hop B. B decrypt the packet with its private key, and obtain the encrypted data and next hop identity to which data is to be send, here it is C's Identity. Upon decrypting the packet, C obtains the identity of D, and sends packet to D. This process is continued until

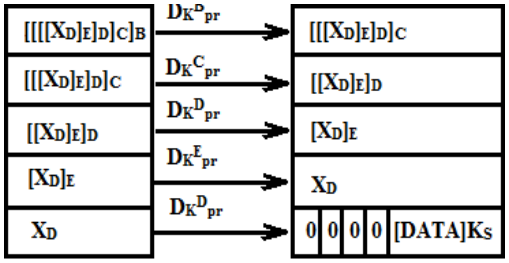


Fig 5: Decryption performed to discover the route

D forwards the packet to E and E returns the packet back to D. When D decrypts the packet, it obtains parity bits in the routing field and an encrypted data field. On seeing the parity bits in routing field, D understands that, the packet is intended to it. Then D decrypts the data in the packet with its secret key, $K^{A}_{s}$ which is shared with source A. The decryption is shown in figure 5.

**Packet Format**

The packet format of "An Efficient Secure Anonymous Communication Protocol based on Destination's Location" is similar to [1], except in some fields. For the succesful communication of source and destination the random forwarder embeds some information into the packet it forwards. It includes, the position of destination node, the TD which is currently selected for routing, the flipping bit (0/1) by each random forwarder, showing the next random forwarder's partition direction. The packet format is shown in figure 6.

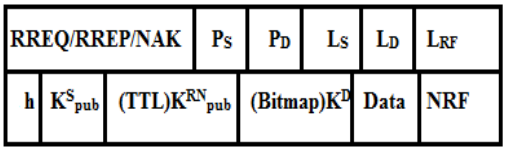


Fig 6: Packet Format

This packet format has similarity with that of [1]. RREQ/RREP/NAK is the universal format, NAK is used for acknowledging the packet loss. In NAK, RREQ/RREP is kept blank. $P_S$ and $P_D$ are the psuedonym of source and destination. $L_{TD}$ is the currently selected temporary destinations coordinate. $K^{S}_{pub}$ is the public key of source. The data field is NULL in NAK. NRF denote the identity of hops through which data is routed from source to destination.

**Anonymity Protection against Attacks**

The one-hop-distance technique used in " An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location can prevent black hole attack. Black hole attack can be defined as the silent discarding of packet by selfish nodes without informing the source or destination. The selfish nodes are those nodes which discard the packets that are not intended to it. This is to save its resources or energy lost in calculating next hop address or forwarding data to next hop. In MANETs employed in military, the black hole attack may results in serious security issues.

In one-hop-distance, the nodes that en route the data includes destination node, ie, the destination node also forwards the data that is intended to it, to other nodes. Consider the example 1, here the routing path with identities of nodes C,D,E,D is encrypted in the order. If B is a selfish node, after decrypting the packet received from A, B understand that it has to send data to next hop C. By carefully analyzing the routing field, B can understand that routing field has now three nodes identities (D, E and D). But B cannot identify which are the three nodes. If B thinks in a manner that, according to one-hop-distance, the node C send data to some other node say X, then X send data to Y and Y return data back to X. So it is not the destination, on thinking so B can discard the packet.

This issue can be avoided by adding parity bits to routing field. So when looking into the routing field, B may gets the number of entries in it. But cannot identify the genuine entries, because routing field is undergone continuous encryption, so it not possible to distinguish the parity bits and the node identity entries. After decrypting the packet, B know the next hop to which data is to be forwarded, here it is C, according to one-hop-distance, there is a probability that the next hop from C can be B and rest of the entries in routing field can be parity bits. So B cannot discard the packet satisfially.

The attacker with information of the communicating nodes can determine the source and destination location. Eventhough each time the source to destination follow different routes, with carefully monitoring the destination location, the intruder can identify the destination node by launching intersection attack. If destination

node is moving slowly as compared to other nodes, the intruder who focus on that location can identify the destination node. But here the destination node send data to another node each time it receives data. So attacker thinks that it is a node that en route data. Here the DoS attack is prevented because, random relay node selection prevent an intruder from intercepting the packet or compromising vulnerable nodes that enroute data.

In timing attack if X's sending time and Y's recieving time have a gap of three seconds ie., (03:00:01, 03:00:04) and (03:00:04, 03:00:07), then after a long observation intruder can identifies X and Y. In order to counter timing attack the constant time interval of two communicating nodes are varied along with notify and go mechanism [1].

**Performance Evaluation**

The network overhead of "An Efficient Secure Anonymous Communication Protocol in MANET based on Destination's Location" is very much less than that of ALERT [1]. The performance graph is shown in figure 7. Detailed performance of two protocols can be obtained from the graph.

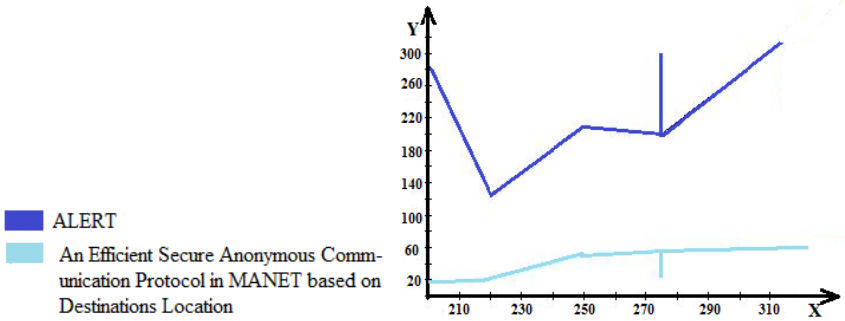


Fig 7: Range Vs Network Overhead

The network overhead of ALERT decreases with the range of two nodes increases, but after a particular range it increases adversly. But network overhead is slightly increased with increase in range, in the case of "An Efficient Secure Anonymous Communication Protocol in MANET based on Destination Location", and is much less than that of alert in all ranges.

## V. Conclusion and Future Work

Security is an important concern of MANET, especially for MANET deployed in military areas. Inorder to make MANET more secure "An Efficient Secure Anonymous Communication Protocol in MANET based on Destinations Location" is proposed, it uses a new concept called one-hop-distance which prevents different types of attacks including black hole attack. This protocol provides anonymity protection to source, destination and route with reduced network overhead and cost.

## Acknowledgement

The authors wish to thank the Management and Principal and Head of the Department (CSE) of Ilahia College of Engineering and Technology for their support and help in completing this work.

## References

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," proc. Int'l Conf. Parallel Processing (ICPP), 2011.
[2] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[3] K.E. Defrawy and G.Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," proc. IEEE Int'l Conf. Networks Protocols (ICNP), 2007.
[4] Y.–C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
[5] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K.Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan.2007.
[6] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug.2005.
[7] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J.Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp.557-570, 2002.
[8] J. Kong, X. Hong, and M. Gerla, "ANDOR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.
[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.
[10] P. Bose, P. Morin, I. Stomenovi&cacute, and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," Wireless Networks, vol. 7, no. 6, pp. 609-616, Nov. 2001.
[11] B. Karp and H.T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in Mobile Computing and Networking, pp. 243-254, 2000.

[12] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad Hoc Networks," pp. 62-68, 2001.
[13] R. Perlman, "Network Layer Protocols with Byzantine Robustness," PhD dissertation, Massachusetts Inst. Of Technology, http:// www.vendian.org/mncharity/dir3/perlman_thesis 1988.
[14] "OSPF with Digital Signatures," IETF RFC 2154, http:// www.ietf.org/rfc/rfc2154.txt, 1997.
[15] S.L. Murphy and M.R. Badger, "Digital Signature Protection of the ospf routing protocol," Proc. IEEE Symp. Network and Distributed System Security (SNDSS '96), P. 93, 1996.
[16] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.
[17] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.
[18] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.
[19] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.