© 2016 IJSRSET | Volume 2 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

MALERT: Modified Anonymous Location Based Efficient Routing Protocol Using Node Categorization Algorithm in MANETs

G. Meenakshi*[1], Kiran. M[2], Praveen. L[3]
*[1]Assistant Professor, Dept. of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India
*[2,3]Student, Dept. of ECE, Velammal Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

Mobile Ad Hoc Networks (MANETs) use anonymous location based routing protocols (ALERT) that hide node identities and routes from outside observers in order to provide anonymity protection rather than relying on hop-by-hop encryption and redundant traffic. The existing anonymous location based efficient routing protocol selects forwarder node in random fashion which may have less power level and memory space which in turn may lead to route failure and not ensure reliability. To offer efficient anonymity protection, Modified Anonymous location based efficient routing protocol selects forwarder node with high power level and high memory space. Node categorization algorithm is used to avoid inside attackers. MALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions to make it difficult for an intruder to detect the two endpoints and route of the transmission. This achieves comparable routing efficiency and provides efficient solution to timing attack than ALERT.

Keywords: Node Categorization Algorithm, MALERT, ALERT.

I. INTRODUCTION

1. Background

RAPID development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyse data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). To offer efficient anonymity protection, Modified Anonymous location based efficient routing protocol selects forwarder node with high power level and high memory space.

Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

II. METHODS AND MATERIAL

1. Literature Survey

In [1], Anonymous routing, Low cost and Resilience to intersection attacks and timing attacks, shows the major contribution. ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. Anonymous geographic routing algorithm is to avoid the explicit exposure of identity and location in communication without compromising the efficiency guaranteed by geographic [5]. The design of the GSPR secure graphic routing protocol is used for authenticating the routing paths taken by individual messages [2]. On-demand location-based anonymous

MANET routing protocol (PRISM) achieves privacy and security against both outsider and insider adversaries. This mainly focuses on privacy aspects of mobility [3]. Geographic forwarding becomes a lightweight routing protocol in favour of the scenarios, where it is ready for use in both ad hoc routing and Internet services [4]. Anew anonymous authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system, which conceals a real identity of communicating nodes with an ability to resist known attacks [8].

2. Work Carried Out

A. Network Configuration

The nodes are created and located in the simulation environment. The nodes are moved from one location to another location. The Random way point mobility model is used in our simulation. The nodes are using Omni-antenna to send and receive the data. The signals are propagated from one location to another location by using Two Ray Ground propagation model. The Priority Queue is maintained between any of the two nodes as the interface Queue. Nodes are selected in random number as per our usage. Mobility of nodes is important as it is in Manet. Each node is given a specific position and movement speed is set. Knowing the past location of the nodes and speed of movement is necessary for better selection of forwarder nodes.

B. Destination Zone partition

Zone position refers to the upper left and bottom-right coordinates of a zone. One problem is how to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D. Using the number of nodes in Z_D (i.e., k), and node densityρ, H is calculated by

$$H - log_2\left(\frac{\rho \cdot G}{k}\right),$$

where G is the size of the entire network area. Using the calculated H, the size G, the positions (0,0) and (x_G,y_G) of the entire network area, and the position of D, the source S can calculate the zone position of Z_D. Assume ALERT partitions zone vertically first. After the first vertical partition, the positions of the two generated zones are (0, 0), $(0.5x_G,y_G)$ and $(0.5x_G,0)$, (x_G,y_G). S then finds the zone where Z_D is located and divides that zone horizontally. This recursive process continues until H partitions are completed. The final generated zone is the desired destination zone, and its position can be retrieved accordingly. Therefore, the size of the destination zone is G/2H. Figure 1 shows various possible ways of zone partitioning between source and destination.

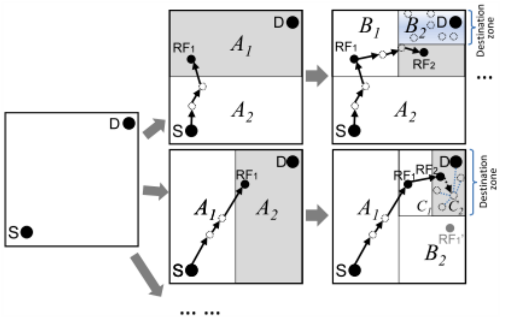


Figure 1 : Zero Partitioning.

C. Forwarder Node Selection

Forwarder node is used for forwarding the data packets. It is necessary to select the efficient forwarder node. Forwarder node should have enough memory space to store the transmitted data and enough power level to forward the received data. Initially, categorising the nodes using node categorization algorithm is performed. Knowing the past location of the nodes and speed of movement is necessary for better selection of forwarder nodes.

D. Node Categorization Algorithm

A Node categorization algorithm is aiming to reduce packet dropper nodes to participate in the route. In every round, for each mobile node u, the destination keeps track of the number of packets sent from u, the sequence numbers of these packets and the number of flips in the sequence numbers of these packets, (i.e., the sequence number changes from a large number such as N_s ¡ 1 to a small number such as 0). In the end of each round, the destination calculates the dropping rate for each node u. Suppose $n_{u,max}$ is the most recently seen sequence number, $n_{u,flip}$ is the number of sequence number flips and $n_{u,rcv}$ is the number of received packets. The dropping ratio in this round is calculated as follows:

$$\frac{n_{u,flip} * N_s + n_{u,max} + 1 - n_{u,rcv}}{n_{u,flip} * N_s + n_{u,max} + 1}.$$

Based on the dropping rate of every mobile node and the tree topology, the destination identifies the nodes that are droppers for sure and that are possibly droppers. For this purpose, a threshold μ is first introduced. It is assumed that if a node’s packets are not intentionally dropped by forwarding nodes, the dropping rate of this node should be lower than μ. Note that μ should be greater than 0, taking into account droppings caused by incidental reasons such as collisions. The first step of the identification is to mark each node with “+” if its dropping ratio is lower than μ, or with “-” otherwise. After all nodes have been marked with “+” or “-“

After categorizing the nodes, a list of good nodes is done. By this, insider attackers and malicious nodes can be avoided. Then best forwarder node which has enough memory space and power level to transmit and receive the data packets is selected.

E. ALERT Routing

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. Given an area, two zones A_1 and A_2 are horizontally partitioned. Then vertically partition zone A_1 to B_1 and B_2. After that, again horizontally partition is done for zone B_2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. The process of this partition is called hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message. Figure 2 shows the forwarding of data packets from source to destination through forwarder nodes and relay nodes.

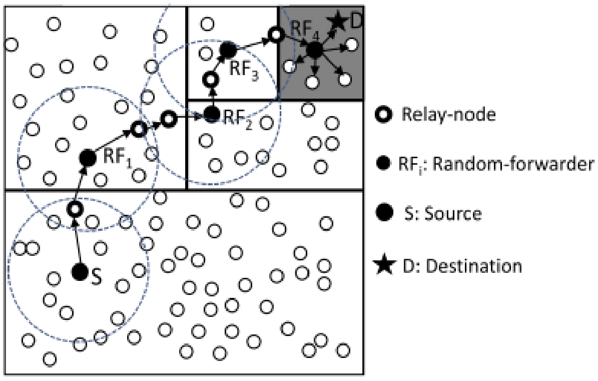
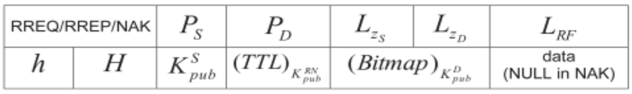


Figure 2 : Alert Routing.

3. Proposed Work

A. Packet Format of MALERT



<table>
<tr><td colspan="2">RREQ/RREP/NAK</td><td>P_S</td><td>P_D</td><td>L_{z_S}</td><td>L_{z_D}</td><td>L_{RF}</td></tr>
<tr><td>h</td><td>H</td><td>K^S_{pub}</td><td>$(TTL)_{K^{RN}_{pub}}$</td><td colspan="2">$(Bitmap)_{K^D_{pub}}$</td><td>data
(NULL in NAK)</td></tr>
</table>

Figure 3: Packet Format for MALERT.

For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet.

1. The zone position of Z_D, i.e., the H^{th} partitioned zone.
2. The encrypted zone position of the H^{th} partitioned zone of S using D’s public key, which is the destination for data response.
3. The current randomly selected T_D for routing.
4. A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF. With the encrypted H^{th} partitioned zone in the information of (2), an = attacker needs very high computation power to be able to launch attacks such as dictionary attack.

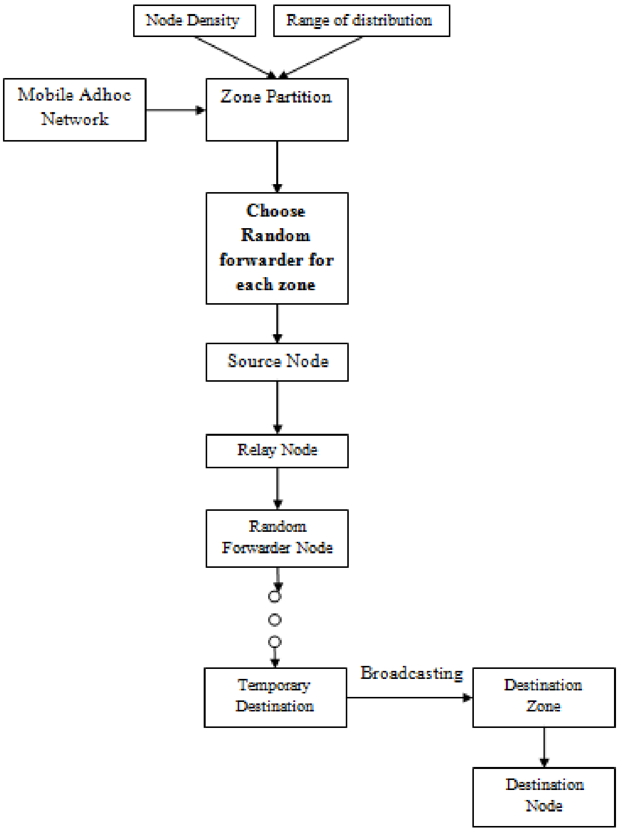


Figure 4: Block Diagram for Proposed Work.

4. Performance Metrics

MANET protocols are the key element in determining many features of wireless networks, such as throughput, Quality of Services (QOS), energy dissipation, fairness stability, robustness which is shown in Figure 5.

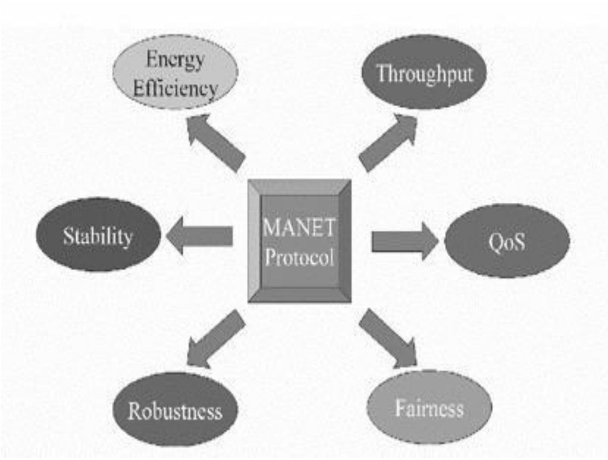


Figure 5: MANET Performance Metrics.

The following are the brief description of metrics:

- Throughput: Throughout is defined as the fraction of raw bandwidth used exclusively for data transmissions .It is not possible to use 100% of the bandwidth for data transmissions due to the unavoidable bandwidth used for overhead (e.g. packet headers, control packet, guard bands) .The objective of MANET protocol is to keep the bandwidth used for overhead as low as possible (high throughput) sacrificing the other objectives.
- QOS: Low delay, high packet delivery ratio, and guaranteed bandwidth are some of the metrics that can define QOS, which is an application dependent concept. For example, QOS for voice packet consists of three packets (i) high packet delivery ratio (ii) low delay (iii) low jitter. Since voice packets are created periodically, MANET protocols should be able to grant periodic channel access for the voice sources without violating the maximum allowable delay for the voice packets after which voice packets are dropped.
- Energy dissipation -Energy efficiency is crucial for light weight batteries operated radios to avoid consuming their limited energy resources. Idle listening is an important dissipation term which can be avoided by switching the radio to a low energy sleep mode. Since in sleep mode a radio cannot receive or transmit MANET protocols have mechanisms to seamlessly put the radio in to the sleep mode and take it back to active mode without violating the efficient operation of the network

III. RESULTS AND DISCUSSION

The performance of the proposed scheme is evaluated by plotting the graph. The parameter used to evaluate the performance is as follows:

- Packet/Data delivery ratio.
- Packet loss ratio.
- Latency.

These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output.

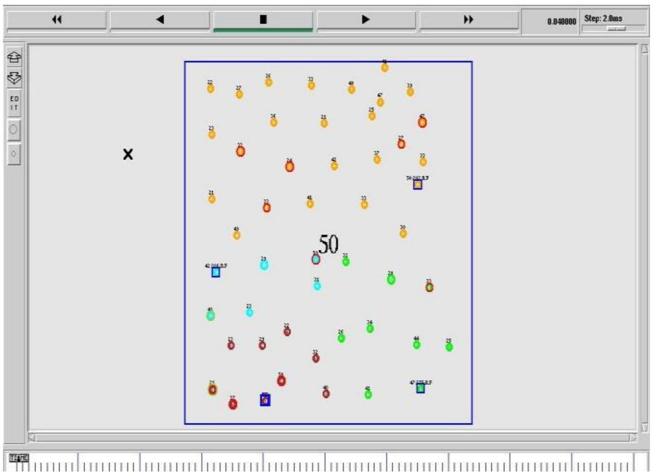


Figure 6 : Network Configuration.

The nodes are created and located in the simulation environment. The nodes are moved from one location to another location.

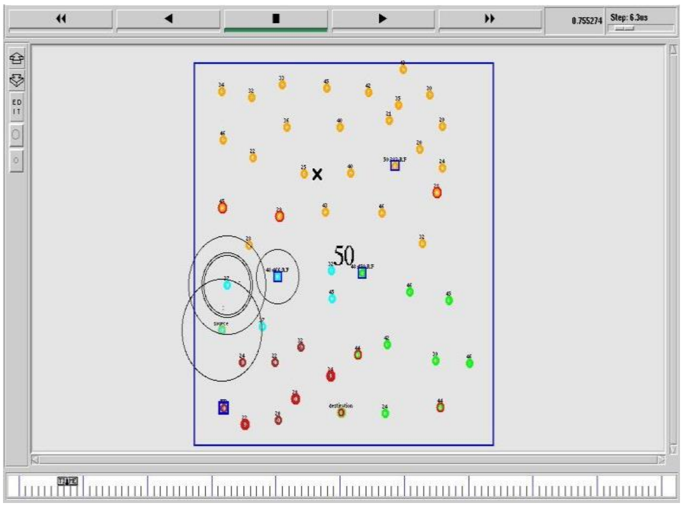


Figure 7 : Transmission from source node to forwarder node.

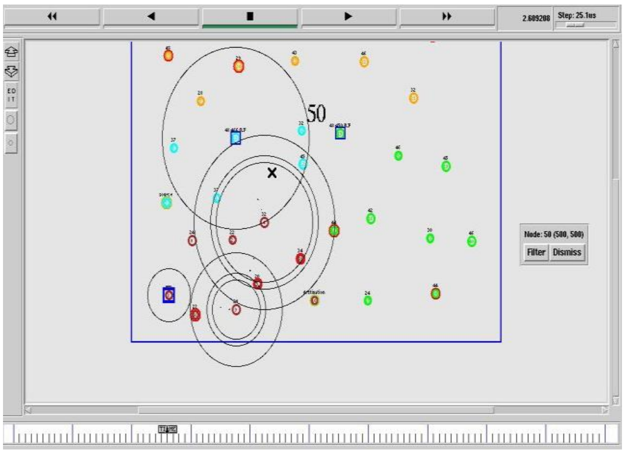


Figure 8 : Forwarder node to Temporary destination Transmission.

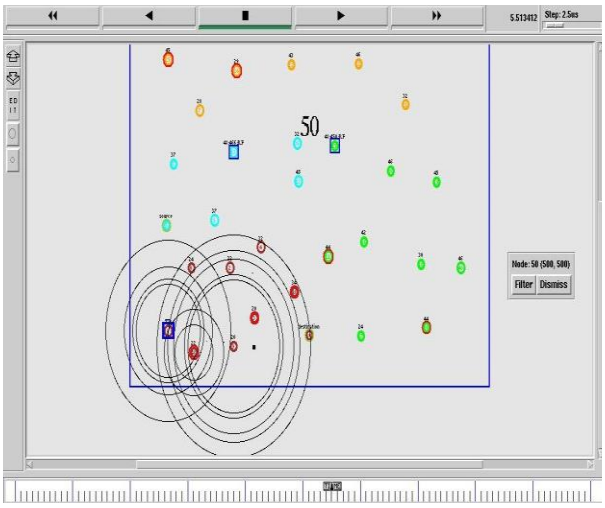


Figure 9 : Broadcasting Data Packets.

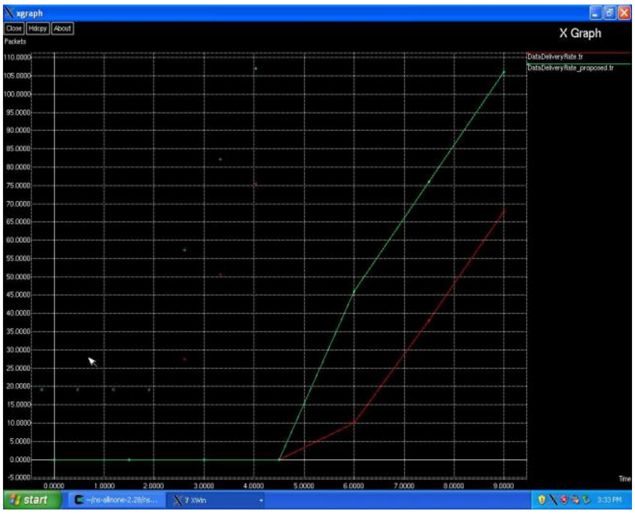


Figure 10: Data Delivery Ratio.

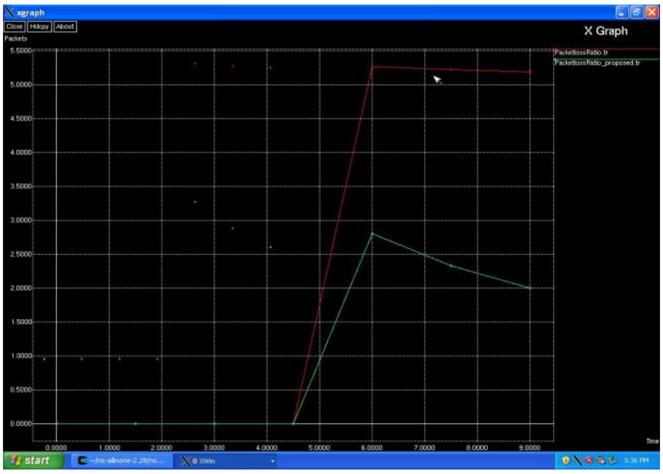


Figure 11 : Packet Loss Ratio.

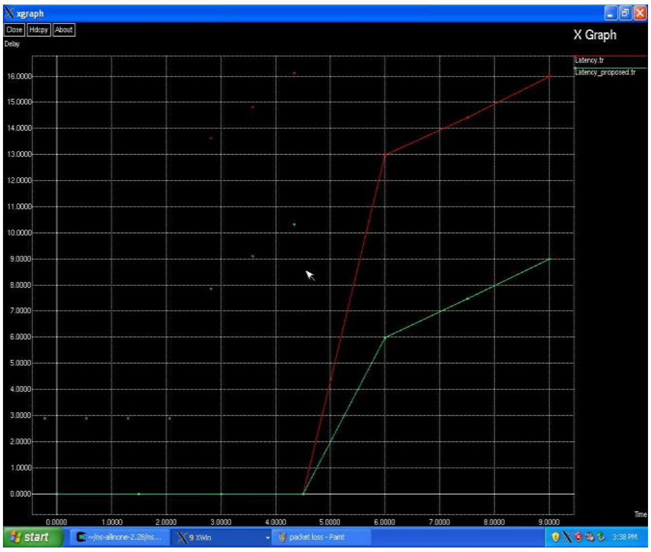


Figure 12 : Latency.

IV.CONCLUSION

MALERT achieves comparable routing efficiency and efficient solution to timing attack than ALERT. It uses efficient forwarder node and relay node selection to make it difficult for an intruder to detect the two endpoints and route of the transmission. It provides low cost and reliable transmission. Future work lies in reinforcing MALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results. By doing so, it can also achieve comparable routing efficiency to the base-line GPSR algorithm. Steps for avoiding routing loops during transmission can be done. Further improvement in efficiency and detection of the various attacks can be done.

V. REFERENCES

[1] Haiying Shen, Lianyu Zhao. (June 2012). "*ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs*", Issue No. 06, vol. 12, ISSN: 1536-1233, pp: 1079-1093.

[2] Vivek Pathak, Danfeng Yao, Liviu Iftode. (2008). "*Securing location aware services over VANET using geographical secure path routing"*, DOI: 10.1109/ICVES.2008.4640905, ISBN: 978-1-4244-2359-0.

[3] Karim El Defrawy and Gene Tsudik. (Dec 2008). "*PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)*", IEEE International Conference on Network Protocols, DOI: 10.1109/ICNP.2008.4697044, ISSN: 1092-1648.

[4] Xiaoxin Wu, Jun Liu, Xiaoyan Hong, and Elisa Bertino.(2008). "*Anonymous Geo-Forwarding in MANETs through Location Cloaking", Anonymous Geo-Forwarding in MANETs through location Cloaking*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 19, NO. 10.

[5] Zhi Zhou and Kin Choong Yow. (May 2006). "*Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy*" International Journal of Network Security, Vol.2, No.3, DOI: 10.1109/ICDCSW.2005.43, ISBN: 0-7695-2328-5, pp: 210–218.

[6] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel. (Feb 2006). "*Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management*" A Consolidated Proposal for Terminology, Version 0.31," Technical Report, 2006.

[7] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto. (Feb 2006). "*An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks*," International Symposium on Applications and the Internet, SAINT 2006. DOI: 10.1109/SAINT.2006.13**,** ISBN: 0-7695-2508-3, 2006.

[8] Tomasz Ciszkowski, Zbigniew Kotulski. (2006). "*ANAP: Anonymous Authentication Protocol in Mobile Ad hoc Network",* 10th Domestic Conference on Applied Cryptography ENIGMA, Warsaw, Poland.