AORPM: Anonymity of Routing Path in MANETs

Arathi K V, Poorvi S Alva, Akshatha K N, Anil Kumar R, Shilpashree S
aarathichandran@gmail.com,poorvisalva@gmail.com,akshathakn03@gmail.com,anilraj330@gmail.com
Dept. Of Computer Science & Engg.,
K.V.G College Of Engineering.,
Sullia,Karnataka,India.,

***Abstract*—Mobile Ad-Hoc Networks (MANETs) are gaining a wide popularity due to the rapid increase in the number of mobile devices. As MANETs are infrastuctreless networks it is vulnerable to malicious attacks. The number of nodes that can take part in communication is not restricted in MANETs and also due to rapid node movement occurance, nodes keeps on changing its location autonomously. The topology of MANETs changes continuously and routing tends to be difficult. It is very much essential to provide anonymous routing in ad-hoc networks to preserve the source, destination and route anonymity. Existing routing protocols cannot provide anonymity to nodes as well as to the route, but the proposed system can ensure anonymity to a greater level. Hybrid key encryption techniques are used to encrypt and decrypt the data and forward the data in a secure manner. Efficient encryption techniques helps to prevent from various types of attacks such as timing attack ,intersection attack etc. we theoretically analyze the proposed system in terms of anonymity and efficiency .Experimental results shows consistency with theoretical results proving AORPM yields better performance and negligible delay.**

***Index Terms*—Anonymity, mobile ad hoc networks, geographic routing**

I.INTRODUCTION

The wide popularity gained by Mobile Ad Hoc Networks (MANETs) due to its self stabilization capacity and error-prone nature had made it one of the preferable network chosen for information sharing as well as communication. Since the use of wireless devices like mobile phones, laptops, PDAs (Personal Digital Assistant) are increasing tremendously in day to day life, the technologies such as wireless LAN (WLAN) is used at its peak. This mainly paved the way for the popularity of MANETs. Due to the independent nature of the MANETs, it is used in numerous applications such as emergency services, commerce, military, entertainment and education. There is no constrain regarding the number of nodes that can be the part of network, as MANETs posses decentralization feature and it act as an open platform welcoming any number of nodes that takes part in communication. But when dealing with the negative aspects of MANETs it is unpleasant to know that it very vulnerable when dealing with external attacks. The external attacks mainly comprises of tampering and analyzing the data and traffic by eavesdropping the communication as well as attacking the routing protocols. As a matter of fact this vulnerability is the main reason which made us to think to develop a new routing algorithm to offer better anonymity for communicating nodes and communicating path.

The anonymous routing algorithms play an important role in MANETs to offer a secure communication. The word anonymity mainly imply that information about nodes that take part in data transmission as well as the details about the route chosen for this data transmission is hidden from the external observers. Anonymity is an inevitable factor when it comes to military application (e.g., communication between soldiers).Consider two soldiers are communicating each other in a battle field, when an enemy tries to eavesdrop this communication, it will be dangerous that enemy can spot the location of soldiers and can attack the respective spots, also enemy can manipulate the crucial information and mislead the soldiers. This situation clearly highlights how much important is the term anonymity. Routing in MANETs is a challenging issue because mobile nodes tend to change its position continuously and create a dynamic topology.

When a comparative study [1] about existing routing algorithms is done, it is known that the Destination-Sequenced Distance Vector (DSDV) [2] creates large routing overhead as well as uses only bidirectional links even though it does not create any nonexistent path. In case of Ad hoc On-demand Distance Vector (AODV) [3] [4] route is created only on demand basis but latency is created every time when a new route is needed. AODV algorithm queues the data packets during the discovery of new routes and these queued packets are sent only after new route is created. A throughput loss is observed in high mobility scenarios as dropping of packets take place quickly due to unstable route selection. When dealing with Location – Aided Routing (LAR) [5], it is understood that this algorithm uses location information to limit the number of nodes to whom the requests is to be done. To obtain the location information Global Positioning System (GPS) is made used. LAR can reduce the scope of root request flood and overhead of rout discovery. The problems arises in this type of routing algorithms as nodes need to know their physical locations and possible existence of obstruction for radio transmission should be taken into account. These algorithms concentrate on routing overhead and routing efficiency.

Coming to routing algorithms that emphasis more on anonymity to a larger extent such as ALARM [6], it cannot protect the location anonymity of source and destination. Most of the anonymous routing algorithms are based on Greedy Perimeter Stateless Routing (GPSR) [7].The GPSR will greedily forward the packets to the nodes evaluating whether it is closer to the destination or not. In this routing the geographical positioning of nodes are considered to decide the routing path. The other constraints of MANETs include limited available resources and complex routing. Existing routing algorithms offer anonymity either to the nodes or to the routing path but yields high cost. But the current paper developed offers high anonymity to both the source node and destination node as well as also to routing path.

II. RELATED WORK

A Survey of Mobility Models for Ad Hoc Network research [10], describes about the survey conducted on mobility models. Mobility of the nodes will either be dependent or independent of other nodes. Mobility model has a greater influence on the performance of the ad-hoc network algorithms. The algorithm is tested on criteria's like limited transmission range, limited buffer space for the storage etc. The performance of the algorithm varies as the parameters of the same mobility model are altered. Mobility pattern is selected based on the data traffic pattern. A Secure On-Demand Routing Protocol for Ad Hoc Networks is proposed[10],this paper presents about the attacks against the routing in ad – hoc networks and also presents the design and performance evaluation of new secure routing algorithm called Ariadne [7]. Ariadne prevents denial of service attacks. It makes use of only highly efficient symmetric cryptographic techniques. This routing algorithm creates routes on demand basis.

Anonymizing Geographic Ad-Hoc Routing [3] for Preserving Location Privacy mainly explains about how geographical routing affects the network in terms of location privacy. Here spacial and temporal cloaking [13] is made used for designing anonymous geographic routing in order to preserve location privacy. Here packets are forwarded using greedy forwarding strategy. Greedy forwarding strategy offers best performance in this type of routing. Location privacy is preserved by dissociating user's information from its identity. The paper does not stress well on factors that affect the location privacy.

Anonymous Communications in MANETs [11], an anonymous neighborhood authentication routing is carried out so that only the nodes that are neighbors of the sending and receiving node will be aware about the data communication. Pair wise secret key techniques are made used to ensure the anonymity. These nodes will never give the details of the communication to any intruder node rather than the secretly paired ones. Currently the efficiency of the routing is compared only with the AODV (Ad-hoc On demand Distance Vector) algorithm. The future work mainly concentrates on experimenting the routing algorithm with other algorithms to proof its effectiveness in providing anonymity.

In the paper about Packet Coding for Strong Anonymity in Ad Hoc Networks, the author tries to establish that packet coding can prevent the attack from global attackers. The packet header as well a packet payload is represented in a different manner so that the combined effect of both will result in an unrecognizable format of packet. So it is difficult for the attackers to obtain the packet information.

The interesting issues such as node identities are addressed by developing an anonymous routing framework by using ALARM [5]. In olden days communication between mobile nodes was mainly based on public identities. But in certain situations preserving node identity and providing anonymity for the routing path is very much essential due to security issues. In ALARM framework, the communication was carried out by spotting the node's current position and based on this position a MANET map is constructed.In order to achieve node authentication, data integrity, anonymity and untraceability certain aspects of cryptographic primitives are made used.In this ALARM node privacy is preserved only if the speed of the mobility of the nodes is comparatively smaller. But the ALARM fails to preserve the node privacy during high speed of mobile nodes as well as it cannot be utilized when the mobility pattern of nodes changes frequently.

PRISM(Privacy – Friendly Routing In Suspicious MANETs) [6], mainly concentrates on privacy features of MANETs. PRISM argues that rather than concentrating on node identities it is better to focus on location information. The paper emphasizes that PRISM can provide privacy and security for both insider and outsider adversaries. PRISM proofs that it is computationally efficient than other routing algorithms which exists. This routing approach does not make use of online servers and node identities as well as no mobility restrictions. The future work of PRISM mainly focuses on extending the routing algorithm for larger environment. Securing Location Aware Services over VANET Using Geographical Secure Path Routing (2008), offers the design of GSPR (Geographical Secure Path Routing).The paper aim to provide location aware services for vehicular ad-hoc networks. GSPR is an infrastructure free routing algorithm that provides a greater security against malicious nodes and its activities. Various experiments have been conducted to examine the overhead of location authentication in ns2 simulator. Experiment yields that the data delivery rate is two times improved even if malicious nodes are increased. Geographical Secure Path Routing uses associative cryptographic one way hash function for security.

Routing Algorithms for MANET: A Comparative Study (2013), a comparative study about different routing algorithms is done. The paper also attempts to group the routing algorithms into different categories like proactive routing algorithms, reactive routing algorithms and hybrid routing algorithms. Routing in MANETs is a challenging issue as it suffers from vulnerability. The paper tries to describe about the features that MANETs should possess, so that routing can be done efficiently. The paper concentrated on DSDV (Destination-Sequenced Distance Vector), OLSR (Optimized Link State Routing Protocol), AODV (Ad – hoc On demand Distance Vector), DSR (Dynamic Source Routing), LAR (Location Aided Routing), ZRP (Zone Routing Protocol).

High Anonymity Protection at a Low Cost in MANETs, thispaper tells that transmitting packet includes source and destination zones rather than positions. Anonymous routing algorithms provide anonymity to source and destination. It mainly uses dynamic hierarchal zone partition and random relay nodes to make it tough for the intruder to detect the two end points. Thus it provides a high anonymity protection at a low cost by the using efficient routing using relay nodes. This routing algorithm is used in multimedia wireless application. It offers better performance.

III.PROPOSED SYSTEM

In the proposed method we mainly perform routing using Greedy Perimeter Stateless Routing (GPSR) protocol. Wireless networks comprise of numerous mobile nodes and these nodes are in dynamic nature. Due to the dynamic nature of mobile nodes, the topology of network keeps on changing and thus routing through these nodes is considered as a challenging issue. It is very much essential that such kind of networks needs an efficient routing mechanism to cope up with rapid changes of network and also to deal when old route collapses. GPSR makes use of correspondence between the geographic positions rather than using graph theoretic notations to find the shortest path. It makes use of position of the nodes to exploit the correspondence and connectivity in wireless network. GPSR uses greedy forwarding to forward the packets to the nodes that are closed to the destination. If the greedy path cannot be determined it goes for perimeter forwarding.

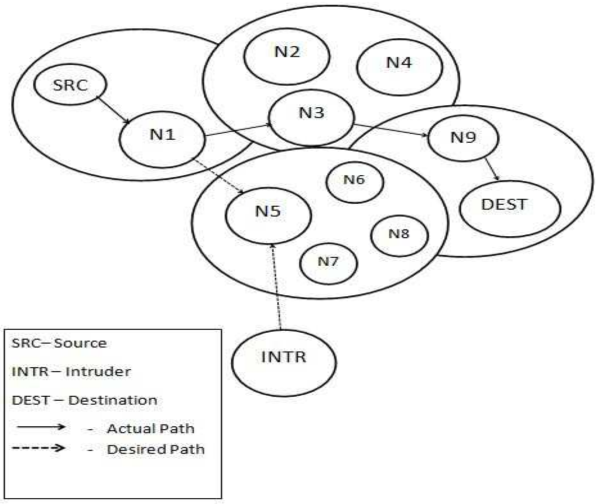

Fig 1: Architectural Diagram

The [illegible] ven in the figure 1.It shows the secure packet transmission between the nodes. The approach proceeds through following ideas. First all possible types of attacks is assumed to take the precautions. The possible types of attacks include timing attack, intersection attack and so on. The area of the experimental set up is evaluated and it is divided into number of zones. The source node as well as the destination node will be settling in different zones. The relay nodes and random forwarders comprises of intermediate nodes. The relay nodes have direct contact with the source and destination nodes. Once the connection is established key server will find the trusted nodes using energy constraints and distance constraints whose explanation is given in below sections. The key server will distribute the keys for encryption as well as for decryption purpose. After this packet transmission will take place in secured path. In the diagram secured path is shown by dotted line and virtual path is shown by straight line. Temporary destination will be assigned to mislead the attacker’s attention. This path is called virtual path.

In order to proceed with secure data transmission he GPSR protocol can be combined with many aspects such as energy level of nodes and other attributes of wireless nodes. The forwarding node will first evaluate the distance between its neighboring nodes .In order to carry out the experimental analysis a boundary value will be initially set.

There will be a certain number of nodes that exist in that boundary value and these node’s energy level will be evaluated to forward the data in a trusted manner .The location of the node is considered as a coordinate in the x-y plane. For example to find out the distance between the two nodes A and B

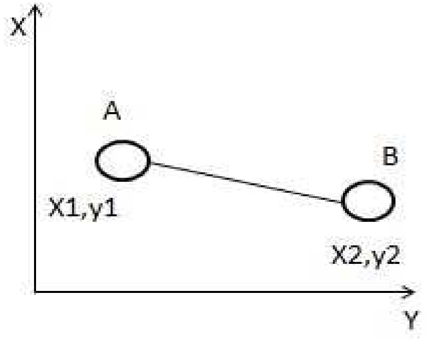

Fig 2: Two nodes in X-Y plane.

Consider node A has (x1, y1) as its coordinates and node B has (x2, y2) as its coordinates. The coordinate indicate its actual location. The distance between the nodes is denoted by d

Thus the packet forwarding occurs to only those nodes which pass both the criterias.The pseudo code of energy basis approach is described below.

```
INPUT: Two nodes that act as a source and sink, Threshold value.
OUTPUT: No of trusted nodes.
INITILIZATION: set the transmission range, set the no of nodes as n, set the threshold as 0.5. Consider two nodes in different position.
[Label the two nodes as i and j]
        If ( i is not eq to j)
Evaluate the distance between the nodes by using the formula for d.
        $d=\surd(x_{2-} x_1)^2 + (y_{2-}y_1)^2$.
Where x and y are the coordinates of the node's location.
        If (d > transmission range)
        {
        Print "no signal received".
        }
        Else
        {
        Check the threshold value.
        If (threshold<0.5)
        {
        Print "trusted node".
        Else
        Print "malicious node".
        }
        }
        Update i  and j until i ≥ n and j ≥ n.Repeat the above steps for all the nodes in the transmission range
```

The distance between the nodes will provide aid to find the shortest path between the nodes. It should be ensured that no two nodes can lie in the same location. The maximum distance between two nodes should be within the transmission range. After evaluating the distance, the energy level which can be called as threshold value of the node is examined. The threshold value is set as 0.5 (only for experimental evaluation and it can be changed). The nodes that possess lesser energy value will be considered as trusted nodes. The nodes that possess higher energy value will not be included in packet transmission as it will be considered as malicious node .After evaluating the trusted nodes the forwarding of packets take place.

The proposed system uses hybrid key exchange algorithm. HYBRID key exchange algorithm uses asymmetric key principles for the distribution of symmetric keys to both parties in a communication network. Key distribution is an important aspect of conventional algorithm and the entire safety is dependent on the distribution of key using secured channel. HYBRID utilizes the public& private key of asymmetric key cryptography to exchange the secret key.

The key server which will issue a public key to all the nodes in the network. The key server stores certain values in the array and it is multiplied by a rand () function to produce the keys. The id based key will be used by the sender node to encrypt the data and the sink node uses private key to decrypt the data. Hashing will be done to further strength the public key encryption technique. The value obtained by multiplying input value with a hash value will be in a complex number such that it is very difficult to analysis the input value. Proper message or data authentication is ensured by using hashing function.

The proposed system can be designed in a step by step way as follows. In the first section attacking models should be studied. In the second step partioning of zones takes place. In the third step key generation and distribution takes place. In the fourth step packet transmission takes place.

A. *Attacking models*

The attacking model should be studied so that packet transmission can be done while avoiding all types of intrusions. The attacking can be in different forms such as timing attack, resilience attack etc. By eaves dropping the adversary nodes the attacker can obtain information about the communication packet and the position of other nodes. Attacking can also be done while analyzing the traffic and storing all the record and historical information about nodes. The attackers can easily find the vulnerable nodes while examining their behaviors. Even though the secure key encryption techniques are used there is always a possibility of key leakage. So a lot of attention is paid towards the attacking models.

B. *Zone partition*

The entire network area which involve in data transmission is portioned into different zones. The number of zones that are created will be dependent on the size of transmission area. There will be always fixed number of zones generated. The source node, destination node and intermediate nodes will be lying in different zones as they lie in different location of network area. The destination zone position is encrypted in packet so that anonymity can be produced. The proposed s randomly selects the intermediate nodes including relay nodes and random forwarders and path for data transmission will be set dynamically.

C. *Key distribution*

The key server will be producing keys and distributing it to the other nodes to strengthen the data transmission. The key server contains number of arrays which contain random numbers. These random numbers are multiplied with a hash value and it is sent to the nodes. The key that is used to encrypt data is id based key and the private key is used to decrypt the data. Hashing will provide more authentications to the nodes. After distributing the keys to the trusted nodes the data is forwarded using user datagram protocol.

D. *Packet transmission*

The packet transmission takes place only through non malicious nodes. The malicious nodes will be misleaded by providing temporary destination .Whenever data transmission takes place temporary destination node is activated so that the attention of malicious node is driven towards the temporary destination node. The packet transmission takes place only through the carefully selected path which will be comprised of relay nodes and random forwarders.

IV. PERFORMANCE ANALYSIS

Performance analysis is simply the process of evaluating how a particular software program is functioning. This process normally begins with how the program loads and what happens when each step in using the program is executed. The object of performance analysis is to ensure the software program is working at optimum efficiency and to identify and correct any issues that may negatively impact that efficiency.The performance analysis is evaluated based on following parameters.

1) Number of nodes.

2) Node mobility.

3) Number of traffic pairs to nodes.

4) Transmission range.

5) Packet delay.

6) Packet dropped.

Here fig 3 represents the performance level of existing system and proposed system. The x-axis represents number of nodes and y-axis transmission range. The proposed system yield much higher performance than existing system. Performance analysis can be evaluated based node mobility and delivery rate as the node mobility increases delivery rate increases. The packet drop and packet delay is very negligible in the new system is up to zero to five performance.

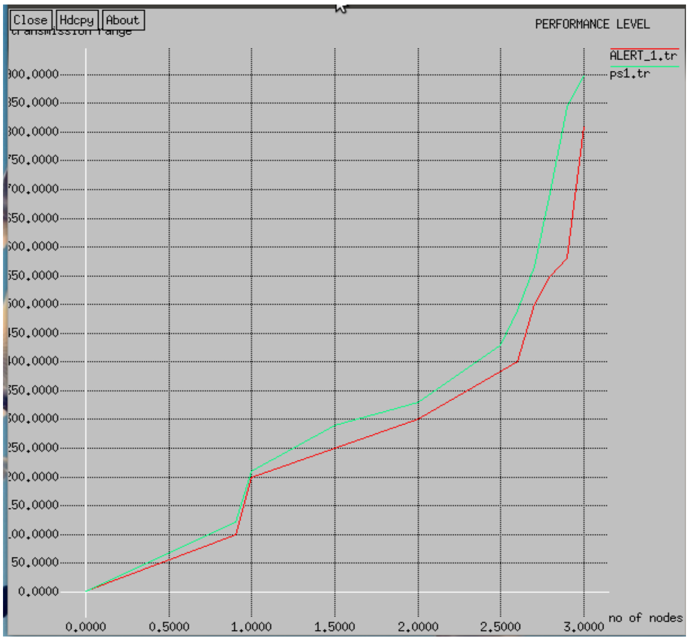

Fig 3:Performance level

The fig 4 shows the performance analysis of proposed system. The graph contains x axis parameter as no of nodes and y axis parameter as transmission range.It is examined that the proposed sytem yields better performance than existing systems.

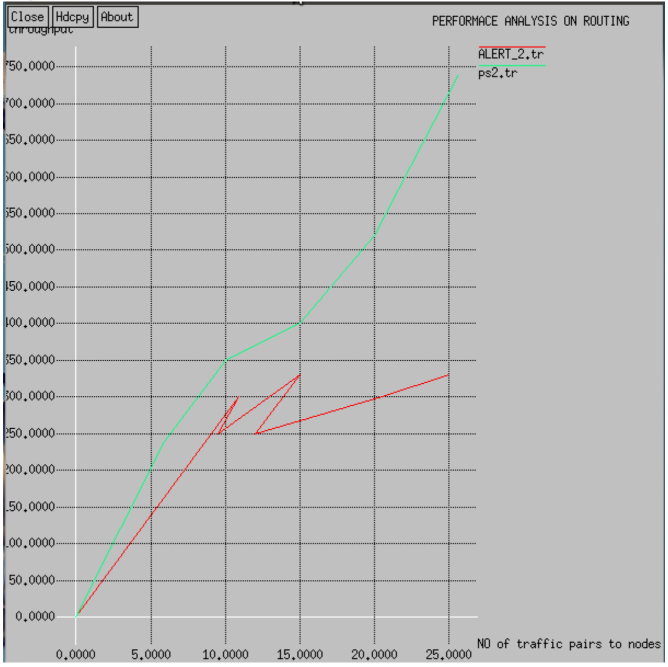

Fig 4:Performance Analysis

The fig 5 and fig 6 shows packet delay and packet dropped. The packet delay and packet dropped is considered in neglible amount.

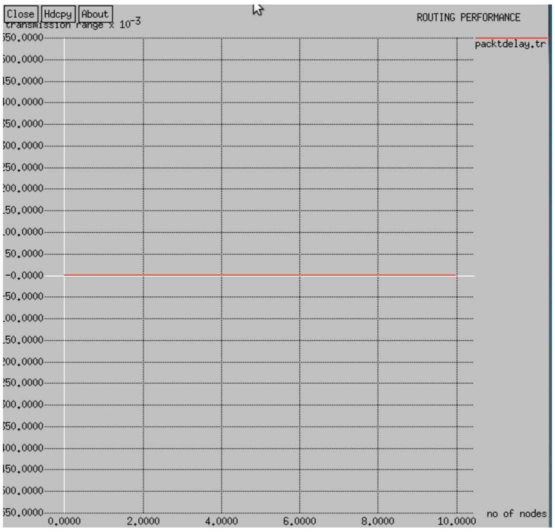

Fig 5:Packet Delay

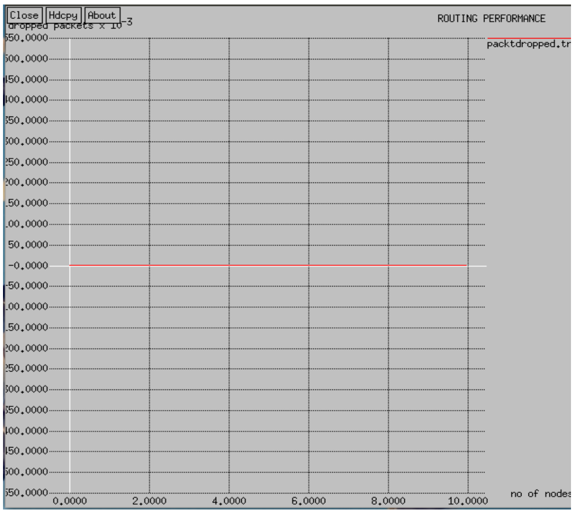

Fig 6:Packet Dropped.

V.CONCLUSION & FUTUREWORK

AORPM serves as a better routing approach compared to other existing routing approaches. Earlier routing approaches give anonymity either to source or to destination or to routing path. But the newly proposed system offers high anonymity to source, destination as well as routing path. It makes use of efficient encryption technique to strengthen the security. Keen mechanisms like distance between the nodes as well as energy constraint of the node etc. are used to evaluate the trusted nodes. Only trusted nodes will be receiving keys and taking part in routing. Temporary destination will be set to mislead the malicious nodes. The newly proposed approach offers high anonymity at low cost and it is resistant to good number of attacks. Future work mainly concentrate on strengthening the routing approach against other unknown and newly creating attacks. From theoretically it is proved that it gives complete protection. From experimentally it is found that it is stable with theoretical analysis.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, “Anonymity,Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,”technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” Proc. Int’l Symp. Applications on Internet(SAINT), 2006.

[3] 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.

[4] V. Pathak, D. Yao, and L. Iftode, “Securing Location Aware Services over VANET Using Geographical Secure Path Routing,”Proc. IEEE Int’l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5] K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf.Network Protocols (ICNP), 2007.

[6] K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf.Network Protocols (ICNP), 2008.

[7] 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.

[8] 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.

[9] 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.

[10] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

[11] Y. Zhang, W. Liu, and W. Luo, “Anonymous Communications in Mobile Ad Hoc Networks,” Proc. IEEE INFOCOM, 2005.