Journal of Theoretical and Applied Information Technology
20th September 2013. Vol. 55 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HYBRID ANONYMOUS LOCATION-AIDED ROUTING PROTOCOL FOR PRIVACY PRESERVING AND AUTHENTICATION IN MANET

[1]Y.V.S.SAI PRAGATHI, [2]S.P. SETTY

[1]Associate professor, Department of Computer Science Engineering
Stanley College of Engineering and Technology for Women,
Osmania University
[2]Professor, Department of Computer Science and Systems
Engineering, Andhra University
E-mail: [1]saipragathi1177@gmail.com

ABSTRACT

In mobile ad hoc networks (MANETs), the existing anonymous routing protocols result in increased overhead as the network size increases. Also, increased delay and inaccuracies are caused when the nodes deployed in the network lags the topology information in prior. In order to overcome these issues, in this paper, we propose a Hybrid Anonymous Location-Aided Routing Protocol (HALARP) for MANETs. This technique utilizes both proactive and reactive mode of anonymous location based routing. The proactive method is applied for the nodes within the pre-defined radius and reactive method is applied for nodes outside the pre-defined radius. When the source wants to transmit the data to the destination, it is executed using suitable encryption technique in secured manner with the help of topology information. By simulation results, we show that the proposed technique offers minimized overhead and delay and increased accuracy.

Keywords: *Mobile Ad Hoc Networks (MANETs), Routing Protocol, Authentication.*

1. INTRODUCTION

1.1 Mobile ad hoc networks (MANET)

Mobile ad hoc networks consist of freely roaming wireless nodes that kindly make up for the absence of fixed infrastructure; that is, the nodes themselves support the network functionality. Mobile ad hoc networks (MANETs) have received great attention in the past few years. Nodes transiently associate with their peers that are within the radio connectivity range of their transceiver and implicitly agree to assist in provision of the basic network services.

It is rapidly deployable and self-organizing configurability have made a MANET very attractive in tactical and military applications, such as the tactical communications in a battlefield, where the environment is hostile and fixed infrastructures are not available or reliable, but fast network establishment, self reconfiguration and security-sensitive operations are necessary.

- The salient features of a MANET are.
- The broadcast nature of the wireless channel.
- The infrastructure less architecture.
- The highly dynamic network topology.
- The limited resources of mobile devices.

All the above salient features of MANET have posed many new challenges in the design and implementation of such a network [1][2].

1.2 Routing Attacks in MANET

The malicious nodes can attack MANET in different ways like sending fake messages several time, fake routing information, and advertising fake links to disrupt routing operations. The confidentiality is not only restricted to user information but also the routing information need to be remain confidential in certain cases. For example, routing information might be valuable for an enemy to identify and to locate targets in a battlefield [2][3].

The current routing attacks and its countermeasures against MANET protocols are discussed below.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Flooding attack: In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume anode's resources, such as computational and battery power or to upset the routing operation to cause harsh degradation in network performance.

Blackhole attack: In blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.

Link spoofing attack: In a link spoofing attack, a malicious node advertises fake links with non-neighbors to interrupt routing operations.

Wormhole attack: A wormhole attack is one of the most difficult and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network.

Colluding misrelay attack: In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to upset routing operation in a MANET [3].

1.3 Authenticated or Secure Routing in MANET

In MANET the secure routing play a very important role because of the absence of a fixed infrastructure. Instead, nodes are transiently associated and cooperate with virtually any node that could potentially disrupt the route discovery and data forwarding operations. The trouble of the route discovery may be an "effective" means to systematically block the flow of data. Adversaries can respond with stale or corrupted route replies, or broadcast forged control packets in order to obstruct the propagation of legitimate queries and routing updates.

All of the routing protocols in MANET depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic achievement in such a setup is that all nodes are well behaving and authentic [2][4].

1.4 Problem Identification

Anonymous Location-Aided Routing in MANETS (ALARM) [5] demonstrates the feasibility of simultaneously obtaining, strong privacy and security properties, with reasonable efficiency. The security includes node/origin authentication and location integrity. Since the protocol is proactive, it incurs large overhead, when the network size grows.

PRISM protocol [9] supports anonymous reactive routing in suspicious location-based MANETs. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. PRISM prevents node tracking from insiders and outsider attacks. Group signature provides additional privacy feature. Group signatures can be viewed as traditional public key signatures with additional privacy features. In PRISM, a node has no a priori topology knowledge so it has to first determine its geographical area of interest and probe it with a route-request message (RREQ), which incurs additional delay and inaccuracy.

To overcome the disadvantages of both these approach, we provide a hybrid Anonymous Location-Aided Routing Protocol for MANETS.

2. LITERATURE REVIEW

Karim El Defrawy et al., in paper [5] consider what it takes to provide privacy preserving secure communication in hostile and suspicious MANETS. They construct a protocol for Anonymous Location-Aided Routing in MANETS (ALARM) that demonstrates the feasibility of simultaneously obtaining, strong privacy and security properties, with reasonable efficiency. In this context, privacy means node anonymity and resistance to tracking. The security includes node/origin authentication and location integrity. Although it might seem that our security and privacy properties contradict each other, they show that some advanced cryptographic techniques can be used to reconcile them.

Mazda Salmanian et al., in paper [6] have demonstrated a decoupling of the maintenance of the Security Association (SAs) from the link state conditions by introducing a timer that defines the lifetime of the SAs, as well as the periodicity of strong authentications. This timer is implemented within a state machine that also manages other aspects of the authentication process. They implement these changes using a Trust-enhanced Routing Table (TRT), an extension of the OLSR routing table.

Jie Liu et al., in paper [7] proposed a framework, in this framework multimodal biometrics are used for continuous authentication, and intrusion detection is modeled as sensors to detect system security state. They formulate the whole system as a partially observed Markov decision process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

considering both system security requirements and resource constraints. They then use dynamic programming-based hidden Markov model scheduling algorithms to derive the optimal schemes for both intrusion detection and continuous authentication.

Quansheng Guan et al., in paper [8] have proposed a topology control scheme to improve throughput by jointly designing upper layer security schemes and physical layer schemes related to channel conditions and relay selections for cooperative communications. The advantage of this approach is that this scheme can substantially improve throughput in MANETs.

Karim El Defrawy et al., in paper [9] have shown how to obtain privacy-friendly on-demand location centric MANET routing. By "privacy-friendly" they give resistance to node tracking by both outsider and insider adversaries. Moreover, this is achieved without sacrificing security.

Raihana Ferdous et al., in paper [10] they have proposed a three threefold approach: to formalize and evaluate trust, to use trust as a basis to establish keys between nodes in MANETs, and to utilize trust as a metric for establishing secure distributed control in MANETs. They define metrics for nodes to establish and manage trust, and use this mutual trust to make decisions on establishing group and/or pair-wise keys in the network. They also review the routing protocols of ad-hoc networks with trust considerations and select Dynamic Source Routing (DSR), a protocol that can be used in distributed ad hoc network settings for path discovery.

Lung-Chung Li et al., in paper [11] have addressed key management in cluster-based mobile ad hoc networks (MANETs). They present a fully-distributed ID-based multiple secrets key management scheme (IMKM). This scheme is implemented via a combination of ID-based multiple secrets and threshold cryptography. It eliminates the need for certificate-based authenticated publickey distribution and provides an efficient mechanism for key update and key revocation schemes, which leads to more suitable, economic, adaptable, scalable, and autonomous key management for mobile ad hoc networks.

Yingbin Liang et al., in paper [12] have proposed to achieve secure communication over MANETs via an approach developed based on information-theoretic security. They have applied the powerful secure coding developed in information-theoretic security to preprocess messages being transmitted through the network to guarantee secure communication in the presence of malicious nodes.

Shengrong Bu et al., in paper [13] have studied distributed combined authentication and intrusion detection with data fusion in such MANETs. Multimodal biometrics is deployed to work with intrusion detection systems (IDSs) to alleviate the shortcomings of unimodal biometric systems. Since each device in the network has measurement and estimation limitations, more than one device needs to be chosen, and observations can be fused to increase observation accuracy using Dempster–Shafer theory for data fusion. The system decides whether user authentication (or IDS input) is required and which biosensors (or IDSs) should be chosen, depending on the security posture. The decisions are made in a fully distributed manner by each authentication device and IDS.

3. PROPOSED SOLUTION

3.1 Overview

In this paper, we propose a hybrid Anonymous Location-Aided Routing Protocol for MANETS. This technique utilizes both proactive and reactive mode of location based routing. The proactive method is applied for the nodes within a pre-defined radius (α). This involves the construction of topology table of the nodes. Then, when the source wants to transmit the data to the destination, it is executed using suitable encryption technique in secured manner with the help of topology information. The reactive method is applied for the nodes outside α . This method involves the route discovery process by broadcasting the route request message and obtaining the route reply from the destined node. Following the route setup, the source node transmits the data to the destination by encryption technique.

3.2 Proposed Technique

To preserve the privacy and authentication, in this paper a hybrid anonymous location aided routing protocol is proposed. It includes the following three phases.

1) Selection of Group Head
2) Proactive Routing Technique
3) Reactive Routing Technique

3.2.1 Selection of Group Head

This phase involves the selection of group head using the following steps

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1) Once the nodes are deployed in the network, each node broadcast the hello message with the node's connectivity (Estimated in section 3.2.4) to its neighbor nodes within 2-hop neighbors. The format of hello message is as follows

Table -1 Format of Hello message			
Node ID	One-Hop Neighbor	Two-hop neighbor	Connectivity

2) After gathering the connectivity value of all the nodes, the node with maximum connectivity is selected as group head (GH). This is illustrated in Figure 1

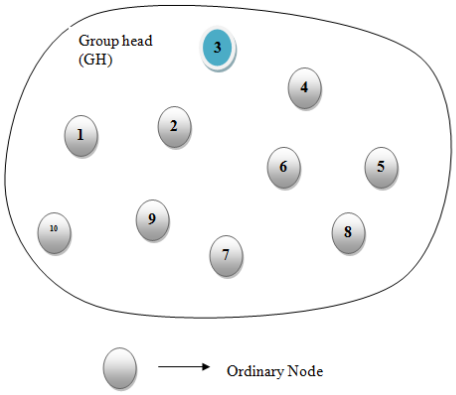

Figure 1 Selection OF Group HEAD

Figure 1 shows the selection of group head. Node 3 (N_3) with maximum connectivity is chosen as group head.

3.2.2 Proactive Routing Technique

Let α be the predefined radius within the group (G)

Let S_{GHi} be the group signature

Let K_{pri} be the private key generated by each node (N_i). (It is required to generate S_{GHi})

Let K_{pui} be the public key revealed to GH alone.

Let K_{si} be the symmetric key

Let (x_i, y_i) be the location coordinates of N_i

Let S and D be the source and destination node respectively.

This technique of proactive routing applies to the nodes within α. The steps involved in this routing technique are as follows

1) Initially each node N_i generates a public and private key pair K_{pui} and K_{pri} at time t. K_{pri} is used by other nodes to encrypt session keys to establish secure channel with N_i.

2) Each N_i broadcasts a location declaration message (Loc_DM) to its neighboring nodes ($Neigh_i$) within α.

$$N_i \xrightarrow{*Loc\_DM} Neigh_i$$

Loc_DM: [ID | (x_i, y_i) | TS | K_{pui} | S_{GHi}]

The format of location declaration message (Loc_DM) is shown in table 2

Table – 2 Format of Loc_DM				
Node ID	Location coordinates (x_i, y_i)	Timestamp (TS)	Public key (K_{pui})	Group Signature S_{GHi}

Upon receiving Loc_DM, each N_i initially executes the following condition.

1) If Loc_DM is already received by N_i
Then
Loc_DM is ignored
End if
2) If new Loc_DM is received
Then
Initially TS of the message is verified
If TS is not valid
Then
Loc_DM is dropped
Else
S_{GHi} is verified for validity
If the verification fails
Then
Loc_DM is dropped
Else
Loc_DM is stored in its cache to construct the topology table and rebroadcasted to its neighbors.
End if
End if
End if

3) When the node gathers the entire Loc_DM, it constructs the topology table of all the nodes within α.

4) If S wants to transmit a data to D, it checks whether D is within R using the topology table. If D is found within R, then S sends a data after performing double encryption process. i.e. Firstly, the data is encrypted with a session key (K_{si}) and then secondly it is encrypted with K_{pui} of previous Loc_DM of D.

$$S \xrightarrow{E[K_{pui}[K_{si}(Data)]} D$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5) D upon receiving the encrypted message retrieves K_{si} and utilizes this key to decrypt the remaining encrypted data.

For example, let us consider figure 1. Within α, the nodes N_1, N_2, N_3, N_4, N_6 exists. When S (N_1) wants to send data to D (N_4), it initially encrypts the data with the session key K_{s1}. This encrypted data is again re-encrypted using the public key K_{pu4} obtained from last Loc_DM of N_4. When the data following the double encryption reaches D, K_{s1} is retrieved and using this key remaining data is obtained.

Secured Data flow: $N_1(S) \rightarrow N_2 \rightarrow N_4(D)$

An intermediate node N_2 upon receiving data verifies whether it is destined to it using the encrypted public key resemblance. If it is not similar, it just forwards the message.

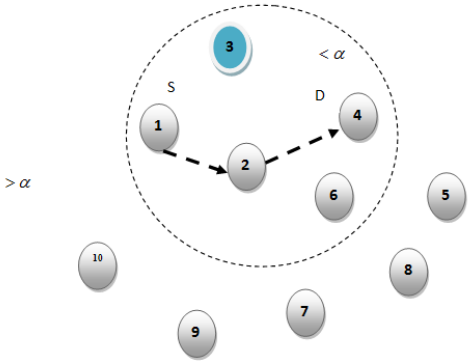

Figure 2 Proactive Routing TECHNIQUE

3.2.3 Reactive Routing Technique

This technique of reactive routing applies to the nodes outside α. If S wants to communicate to any destination outside α, it switches into reactive mode. The reactive routing technique is demonstrated using the following algorithm.

1) If S wants to transmit the data outside α, it sends R_Req message to the nodes outside α.

The format of RREQ message is shown in table 3

Table – 3 Format of RREQ

Node ID	Location [α, (x_i, y_i)]	Timestamp (TS)	Public key (K_{pui})	Group Signature S_{GHi}

(2) Each N_i upon receiving R_Req message verifies three scenarios in sequential order

i) TS validity and
ii) Prior arrival of R_REQ to the node (Note 1)
iii) S_{GHi} validity in sequential order.

If above three scenarios are satisfied

Then

N_i caches the message and rebroadcasts it to the neighboring nodes.

Else

R_Req is dropped.

End if

3) D upon receiving the R_Req generates R_Rep which contains the R_Req, session key K_{si}, location information, and S_{GHi} of all fields. R_Rep is encrypted using K_{pui} and broadcasted in the reverse direction of R_Req.

4) Each node N_i upon receiving R_Rep executes the following conditions.

i) If N_i does not contain R_Req in its cache
Then
R_Rep is dropped
End if
ii)If N_i contains R_Req in its cache and R_Rep is already been processed
Then
RREP is dropped
End if
iii) If N_i contains R_Req in its cache and received R_Rep is new
Then
N_i stores the R_Rep information in its cache and rebroadcasts it towards S.
End if

Thus each N_i contains R_Req, R_Rep and TS as main entries in its local cache.

5) S upon receiving R_Rep verifies timestamp validity, location information and S_{GHi}. If the received information is valid, then S decrypts the K_{si} and location offered by D. This key is further utilized for message authentication. Upon receiving invalid R_Rep, S simply discards the message.

6) S then uses K_{si} to encrypt the data that it desired to transmit to D using the established route.

7) In case, any link in the established route breaks, the corresponding node sends an error message to S. The source then discovers an alternate route.

Note: 1) N_i checks whether R_Req has already been received by looking into its local cache where all the R_Req information is stored.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Advantages of the proposed approach

- It provides node/origin authentication and location integrity.
- Supports anonymous reactive routing in suspicious location-based MANETs
- Group signature provides additional privacy feature.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

We use NS-2 [14] to simulate the proposed HALARP protocol. In this simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. In this simulation, the mobile nodes move in a 500 meter x 500 meter region for 50 seconds simulation time. The node speed is fixed as 5m/s. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in table 4.

TABLE 4
SIMULATION PARAMETERS

No. of Nodes	100
Area Size	500 X 500
Mac	802.11
Routing Protocol	HALARP
Simulation Time	50sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Speed	5m/s
Rate	100Kb
Attackers	2,4,6,8 and 10.
Transmission Range	250,300,350 and 400m

4.2. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Delay: It is the total amount of time taken by the packet to receive the receiver.

Drop: It is the number of packets dropped during the data transmission.

Throughput: It is the total number of packets received by the receiver.

HALARP is compared with the PRISM [9] protocol. The simulation results are presented in the next section

4.3 Results

A. Based on Range

Initially, we vary the transmission range as 250,300,350 and 400m.

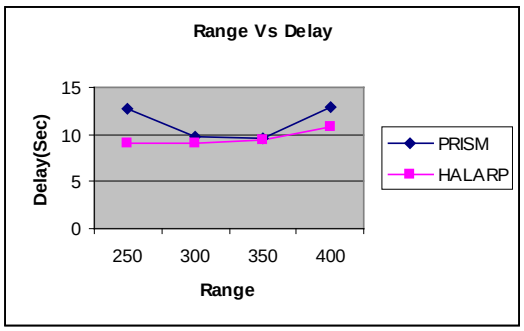

Figure 3: Range Vs Delay

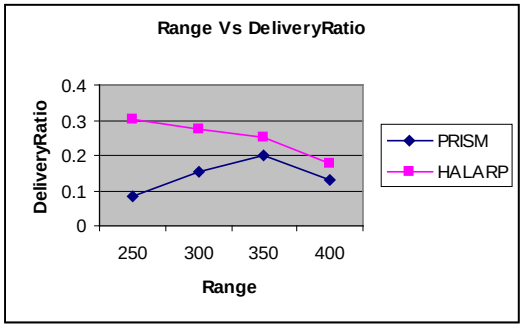

Figure 4: Range Vs Delivery Ratio

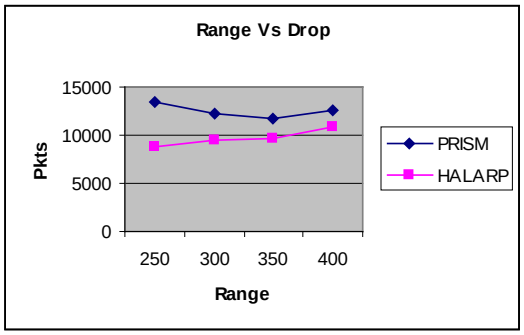

Figure 5: Range Vs Drop

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

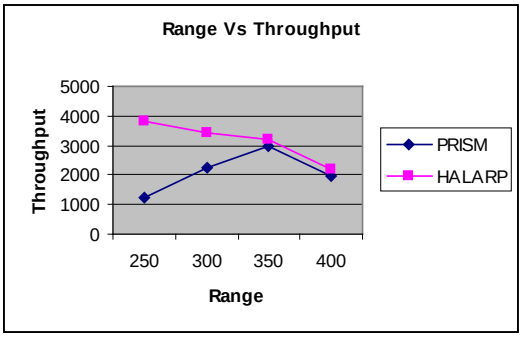

Figure 6: Range Vs Throughput

From figure 3, we can see that the delay of our proposed HALARP is less than the existing PRISM protocol.

From figure 4, we can see that the delivery ratio of our proposed HALARP is higher than the existing PRISM protocol.

From figure 5, we can see that the drop of our proposed HALARP is less than the existing PRISM protocol.

From figure 6, we can see that the throughput of our proposed HALARP is higher than the existing PRISM protocol.

B. Based on Attackers

Next, we vary the number of attackers as 2,4,6,8 and 10.

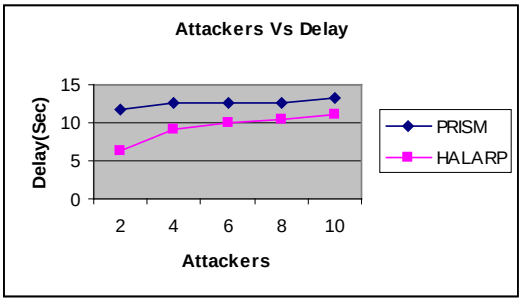

Figure 7: Attackers Vs Delay

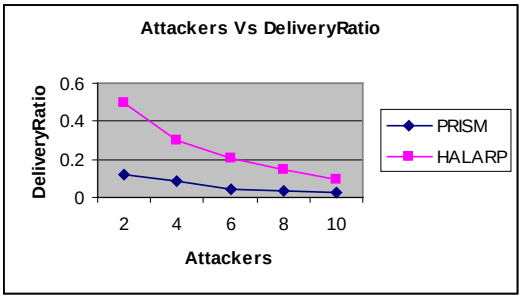

Figure 8: Attackers Vs Delivery Ratio

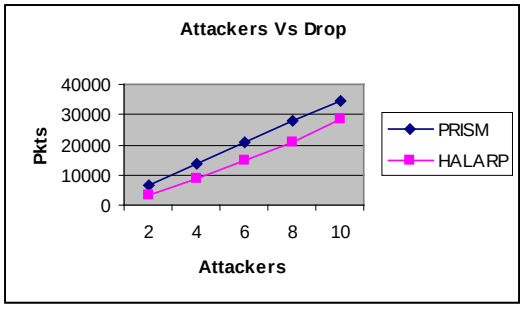

Figure 9: Attackers Vs Drop

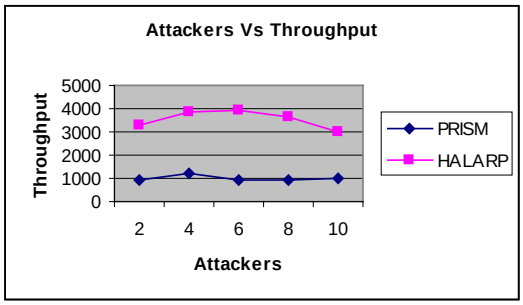

Figure 10: Attackers Vs Throughput

From figure 7, we can see that the delay of our proposed HALARP is less than the existing PRISM protocol.

From figure 8 we can see that the delivery ratio of our proposed HALARP is higher than the existing PRISM protocol.

From figure 9, we can see that the drop of our proposed HALARP is less than the existing PRISM protocol.

From figure 10, we can see that the throughput of our proposed HALARP is higher than the existing PRISM protocol.

5. CONCLUSION

In this paper, we have proposed a hybrid Anonymous Location-Aided Routing Protocol for MANETS. This technique utilizes both proactive and reactive mode of location based routing. The proactive method is applied for the nodes within a pre-defined radius (α). Initially, this method involves the construction of topology table of the nodes. Then, when the source wants to transmit the data to the destination, it is executed using suitable encryption technique in secured manner with the help of topology information. The reactive method is applied for the nodes outside α. This method involves the route discovery process by broadcasting the route request message and obtaining the route reply from the destined node.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Following the route setup, the source node transmits the data to the destination by efficient encryption technique. By simulation results, we have shown that the proposed technique offers minimized overhead and delay and increased accuracy.

REFERENCES

[1] Wenjing Lou, Wei Liu, Yanchao Zhang and Yuguang Fang, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks", *Wireless Netw* (2009) 15:279–294

[2] Panagiotis Papadimitratos and Zygmunt J. Haas, "Securing Mobile Ad Hoc Networks", 2003

[3] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, volume (2) issue (3) 2006

[4] Turkan Ahmed Khaleel and Manar Younis Ahmed, "The Enhancement of Routing Security in Mobile Ad-hoc Networks", *International Journal of Computer Applications* (0975 – 888), Volume 48– No.16, June 2012

[5] 5. Karim El Defrawy and Gene Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", *Mobile Computing, IEEE Transactions on* 2011 , Page(s): 1345 - 1358

[6] Mazda Salmanian, Jiangxin Hu, Li Pan, Peter C. Mason and Ming Li, "Supporting Periodic, Strong Re-authentication in MANET Scenarios", *the 2010 military communication conference- unclassified program - cyber security and network management*

[7] Jie Liu, F. Richard Yu Chung-Horng Lung, and Helen Tang, "Optimal Combined Intrusion Detection and Biometric-Based Continuous Authentication in High Security Mobile Ad Hoc Networks", *IEEE Transactions On Wireless Communications*, Vol. 8, No. 2, February 2009

[8] Quansheng Guan, F. Richard Yu, Shengming Jiang and Victor C.M. Leung, "A Joint Design for Topology and Security in MANETs with Cooperative Communications", *This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings*

[9] Karim El Defrawy, Member, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", *IEEE Journal on Selected Areas in Communications*, Vol. 29, No. 10, December 2011

[10] Raihana Ferdous, Vallipuram Muthukkumarasamy and Abdul Sattar, "Trust Formalization in Mobile Ad-Hoc Networks", *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*

[11] Lung-Chung Li and Ru-Sheng Liu, "Securing Cluster-Based Ad Hoc Networks with Distributed Authorities", *IEEE Transactions on Wireless Communications*, Vol. 9, No. 10, October 2010

[12] Yingbin Liang, Vincent Poor and Lei Ying, "Secrecy Throughput of MANETs Under Passive and Active Attacks", *IEEE Transactions On Information Theory, Vol. 57, No. 10, October 2011*

[13] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks", *IEEE Transactions On Vehicular Technology*, Vol. 60, No. 3, March 2011.

[14] Network Simulator: http:///www.isi.edu/nsnam/ns