# Route Challenging Scheme Using Friend Based Rating in MANETs

S. Shantha Meena [#1], V.S. Shankar Sriram [*2]
School of Computing, SASTRA University [#1]
Thanjavur, Tamil Nadu, 613401, India
shanthameena.s.2@gmail.com
School of Computing, SASTRA University [*2]
Thanjavur, Tamil Nadu, 613401, India
sriram@it.sastra.edu

***Abstract*— Security and Route identification are the major challenges in MANETs. Existing neighbour based routing algorithms provide route based on the quantity of data transferred [1] which may result in congestion. This is because the route having higher amount of transaction is preferred every time. In this paper we propose a Friend Based Routing algorithm [FBRA] for solving this problem. Here, the appropriate route is found not only based on the quantity of data transferred but also considers RSS and RTT. For providing re-authentication to the nodes in the network, FBRA uses Zero-Knowledge Protocol. The main advantage of this method is providing enhanced security and distinguishes the malicious nodes from the trusted nodes in the network.**

**Keywords - MANET, Routing, ad-hoc, Re-authentication, Friend-based, FBRA Scheme.**

## I. INTRODUCTION

In the locations like combat zone and calamity area, there may not be any infrastructure. In the Holocene years, technology for communication has major improvements. Node mobility plays an important role, because people need communication everywhere and every time. For these kinds of areas, mobile ad-hoc networks called MANETs are very useful. MANETs depends upon the collaboration of the participating nodes, because it consists of many wireless nodes. Depending upon the number of nodes that collaborate, the effectiveness of the MANETs is estimated. In MANETs, there is no fixed topology. Also MANETs have limited network bandwidth, less memory and low power batteries. Each node in a MANET has the route information within the network.

Routing protocols are of two types [2]: Proactive and Reactive protocols. Reactive routing protocols are on-demand. They will find route to destination from source when it is necessary. But proactive routing protocols are periodic. They will find routes periodically for the nodes. It leads to overhead. Reactive routing consists of two steps. In first step, source sends the route request message to the network. After it reached every node, it replies with route. In second step, if any node in the route is damaged, then the route is altered by sending error message to the source.

Major threats in the form of selfish nodes and malicious nodes [3] result in the loss/modification of packet transferred. Selfish nodes do not forward packets to other nodes for saving its own energy. But it does not directly have an effect on the other nodes in the network. Some nodes do not care about their power but have an effect on other nodes due to its misbehaviour. There is some susceptibility in MANETs. They are portability, air medium, limited resources, dynamic nature, and consistency.

One solution for mitigating attacks from selfish nodes and malicious nodes is secured routing. Secured routing means that it provides the accurate routing information. Few protocols like ARAN [4] and ARIADNE [5] provide secured routing. But the limitation is that the protocols do not address a concrete methodology to re-authenticate nodes that left network and wish to rejoin the same network.

In this paper we intend to propose a FBRA for secured routing and re-authentication of nodes that wish to rejoin the network. This mechanism employs Zero Knowledge Protocol [ZKP] and can find the malicious nodes by calculating trust rating for each and every node in the network. Rating calculation is based on the three parameters called Round Trip Time [RTT], Rating for Data Transfer [RDT] and Received Signal Strength [6] [RSS]. Then the sharing and routing process are same as in the FACES [1].

The rest of the paper discuss about the following : section 2 briefly analyse the previous works done on routing in MANETs, section 3 described the FBRA algorithm, section 4 represents the simulation results provided by FBRA, section 5 concludes this paper.

## II. RELATED WORK

T.Haniotakis,S.Tragoudas and C.Kalapodas[7] proposed a Disjoint Multipath Routing for secure data forwarding involving two nodes. Here, the method is employed with public key in the packet itself. In this process, the message is divided into parts. Then the encrypted parts only send to the node through diverse lanes.

Only after all the parts are received, the node is able to decrypt the packet. Another property of this method is shortest path between the nodes. The main concern is set to the nodes based on the number of links they have. The advantage of this method is the interrupt needs all the parts to get the novel message.

The method proposed[8] by Zouridaki et al. (2006), every node in the ad hoc network needs to find the confidence rating of others to provide consistent routing. Here it needs to unite the two faith information. One is gained independently and another one from the suggestion of others. In [9] On-demand Multicast Routing Protocol(Lee et al.), a source initiates packet request occasionally. The receiver responds to it. Here, the improvement shows that the delivery ratio is high. The drawback is increase of control overhead based on network size.

In 2011, Sanjay K. Dhurandher et al. proposed the FACES [1] algorithm that is used to provide a highly secure routing among nodes. It employs the ratings for every node in the network based on the trust level. And also having challenges for verifying the nodes. In this paper, there are four stages. First stage for verifying the nodes by making challenges. Second stage for finding the trust levels for all nodes in the network. Third Stage for sharing the friends list from other nodes. Fourth stage for providing routing based on the ratings calculated. The drawback in this scheme is highly rated path getting more packets for forwarding leading to congestion.

Kimaya Sanzgiri et al. proposed ARAN [4] provides security for routing based on faithful record from server. For finding routes, route detection message is sent to all nodes in one-to-many form. Target node responds to the source. Here authentication is done on each and every node in the path for forwarding as well as in reverse manner. These rules are simple and cost for performance is minimum too.

In 2011, George C. Hadjichristofi et al. planned and employed a new ad-hoc routing protocol [10]. To develop routing decisions, this protocol uses connectivity and quality of link. Key management technique affords secure paths through which packet routing and control messages of topology takes place. Also it uses monitoring techniques.

## III. PROPOSED SYSTEM

The proposed system uses a four step mechanism. Step 1 addresses the process of authentication and re-authentication. Step 2 calculates the rating value. Step 3 shares the friend list. Step 4 explains the on-demand routing. Figure 1 shows the architecture of FBRA.

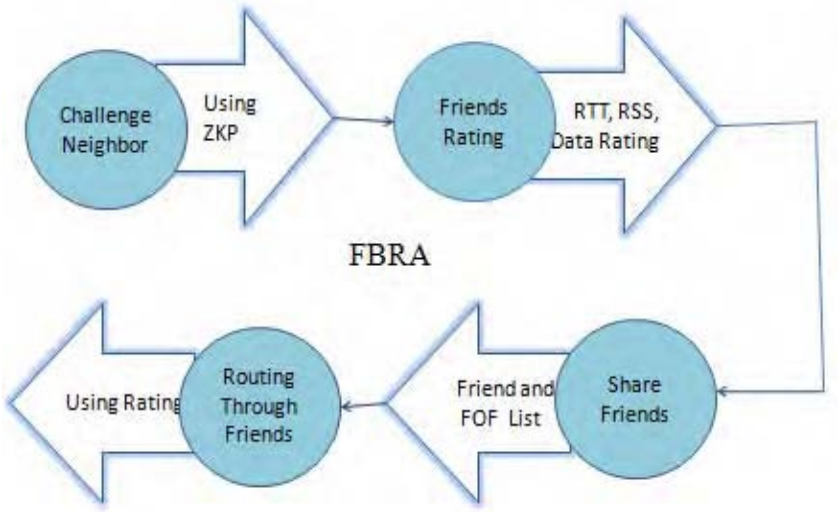


Figure 1 : FBRA Architecture

The purpose of re-authentication is to avoid intruder attacks while rejoining the network. Friend rating calculates the trust level of nodes and isolates malicious nodes. Friend sharing propagates the trusted nodes throughout the network. Routing through rating avoids the involvement of routing via malicious node.

### A. *Methodologies*

*Step 1: Neighbour Challenging*

Neighbour Challenging means checking neighbours whether they are trusted or not. An incoming node is integrated into an existing network by providing assurance in means of challenge. If a new node arrives, it gets authenticated by the existing nodes in the network.

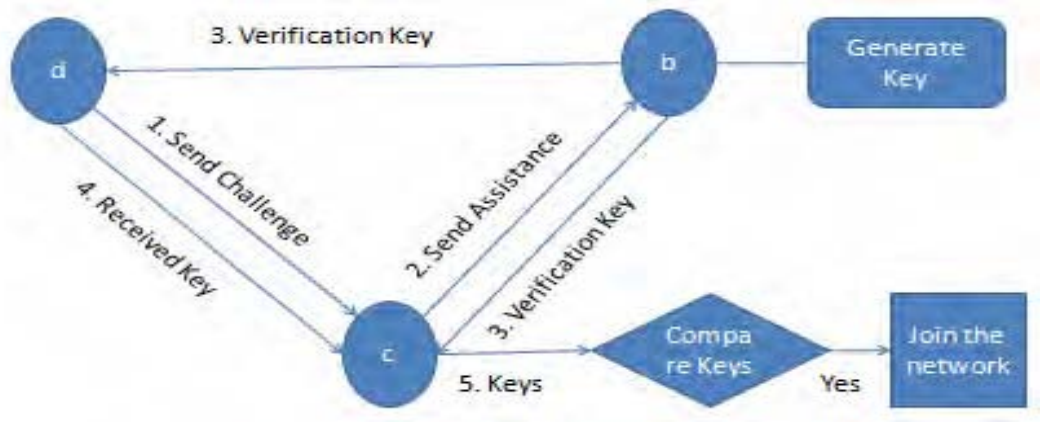


Figure 2: Key Verification

By challenging the existing node in the network, the challenged node assists another node. The assist node generates the key and sent to the both challenging and challenged node. If a challenging node is an assured node, it sends the received key to the challenged node. After a successful verification a new node is integrated into the network.

Figure 2 shows the key verification process [1]. New node'd', challenges the existing node 'c'. Node 'b' is assisted by 'c'. Then 'b' sends verification key to both nodes and 'd' forwards it to 'c'. Node 'c' compares keys. After successful comparison, node 'd' joins in the network.

By re-authentication process, the relived node rejoins in the network. For this, FBRA uses Zero Knowledge Protocol [ZKP] that contains four set of rules. The 4 steps are explained as follows.

In step 1, p1 and p2 are two prime numbers generated by A. A ask B to find the F(x) value, where x is the maximum of p1 and p2. In step 2, r1 and r2 are two random numbers generated by A. A ask B to find log (r1,r2). In step 3, x1 is an integer generated by A. A ask B to find sin (-x1) value. In step 4, A generates three numbers a1, b1, c1 and ask B to find $a^2$ value. Then find the probability for received answers. Based on the probability, A rejoins B. The above operation is explained briefly in section 3.2.

*Step 2: Friends Rating [FR]*

Friend rating means that finding trusted rate for friend nodes. Consider three parameters namely: Round Trip time [RTT], Rating for data transfer [RDT] and Received Signal Strength [RSS]. Based on these parameters, credence rate is determined. Rating for data transfer is calculated based on the amount of data transmitted efficiently for a particular node. The last five transactions are considered. The equation for finding rating for data transfer is:

$$RDT[i] = RDT[i-1] + RDT[i-2] + RDT[i-3] + RDT[i-4] + RDT[i-5] / 5.$$

The equation for finding Round Trip Time is:

$$RTT = (\alpha * old\_RTT) + ((1- \alpha) * new\_RTT).$$

By combining these three parameters, the rating for friends is determined. Using the following equation the FR is calculated.

$$FR = RTT + (RSS / RDT).$$

*Step 3: Friends Sharing*

Friend sharing is the process of sharing friend list**.** By friend sharing request, all the nodes share their friend list in a network. Consider the two nodes S and M needs to share their friends list. This process follows the steps given below: At first step, after the network initialization process and friend forming process, if node S has node M in its friends list, but a particular node in M is not in friend list of S. Particular node from M is added to S by assuming its rating as zero. Then if both S and M has same set of friends, keeps the rating as it is.

*Step 4: Routing through Rating*

Routing [1] is an on-demand and source initiated process. Route Request message is sent and upon receiving the response in the form of Route Reply message, the best route is evaluated depending on the rating of every node. After the data transmission, acknowledgement is received with number of packets. If both number of packets sent and received matches then the RDT is increased. Routing is taking place only through the trusted nodes.

*B. Algorithm*

Join of New Node:

n - Network, k - key, N – node, E(N) – existing node.

If N(d) needs to join n;
Then N(d) communicates N(a) in n;
To authenticate N(d), N(a) needs the assistance of e(N)
Process e(k) → a(k) & d(k)
If d(k) == a(k)
Then d joins n

Re-authentication Using ZKP:

P – probability, P1, P2 - prime number, R1, R2 - random number, X1 – integer, a1,b1,c1 – random number
A generates p1, p2
A → B: F(x) = ?, where x = max (p1, p2)
B → F(x) → A
A calculates p(f(x))
A generates r1, r2
A → B: log(r1,r2) = ?
B → log (r1,r2) → A
A calculates p(f(x))
A generates X1
A→ B: Sin(-X1) = ?
B → Sin(-X1) → A
A calculates p(f(x))
A generates a1,b1,c1
A → B : $a^2$ = ? Where (a1,b1,c1)
B → $a^2$ → A

Routing through Rating

dr - data rate, n – node, RR - Route Request, R – Rating, F(L) - Friends List, i,j - any nodes in n
For € n calculates {
dr calculated dt(n)
RTT is calculated for n
RTT=(α * old_RTT)+((1-α)*new_Round_Trip_Time)
RSS calculates for n
distance= $Rss^2$/quality * 1.92 }
For(€ n calculates Rating ){
R(n)=RTT+(distance/dr) }
n shares F(L) with € n
n(i) shares F(L) with n(j);
Any n(i)→F(L) is not in n(j)→ F(L) then
Add n(i)→ F(L) to n(j)→ F(L) assume dr(n)=0
n(T) take place then RR→ sent.
Evaluate € route by R
From S to D
Choose r using R
If( dl is not in n) then increase dr
Else
Initiate Sequential Challenge
If detect data loss then
Remove n from F(L)

1) *Explanation*

First step is joining of a new node in the network ‘n’. If a new node‘d’ wants to join in the ad-hoc network, it will need the authentication from the node ‘a’ in the network. So it will make a challenge to node ‘a’. Node ‘a’ needs the assistance of any existing node ‘e(N)’ in the network for authentication. Then the key ‘k’ is generated

and sent to‘d’ & ‘a’. After that new node send the key to ‘a’. It will compare the both keys ‘d(k)’ & ‘a(k)’. If they are same, then node‘d’ will be added to the network.

Second step uses ZKP for re-authentication of the node that wishes to rejoin in the network. It uses four rules for re-authentication. ‘A’ is the node in the network and ‘B’ is node needs to be authenticated. In that first rule, ‘B’ needs to find the function ‘F(x)’ which is already given to the node when it is present in the network. It finds the result and brings it back to ‘A’. Then ‘A’ finds the probability of that answer with the answers already in it. Likewise, all the four rules are verified.

Third step is for finding the belief rating of each and every node. For that estimation, equations mentioned in the algorithm are used for finding RSS, RTT and RTD. Using that route is determined and starts forwarding the packets.

## IV. RESULTS AND DISCUSSION

The execution environment was Network Simulator version 2, Fedora on an Intel Core2Duo processor, 4 GB RAM machine. The simulation result for the proposed algorithm is shown in figure 3 & 4. Figure 3 shows that nodes A,B,C,D are existing nodes and a new nodes wishes to join the network. First new node tires to connect with node A. Node A gets the assistance of node B. Node B sends key to A node and a new node. Then node A checks the key from new node for authentication. Figure 4 shows that the routing takes place from source to destination which has high rating value.

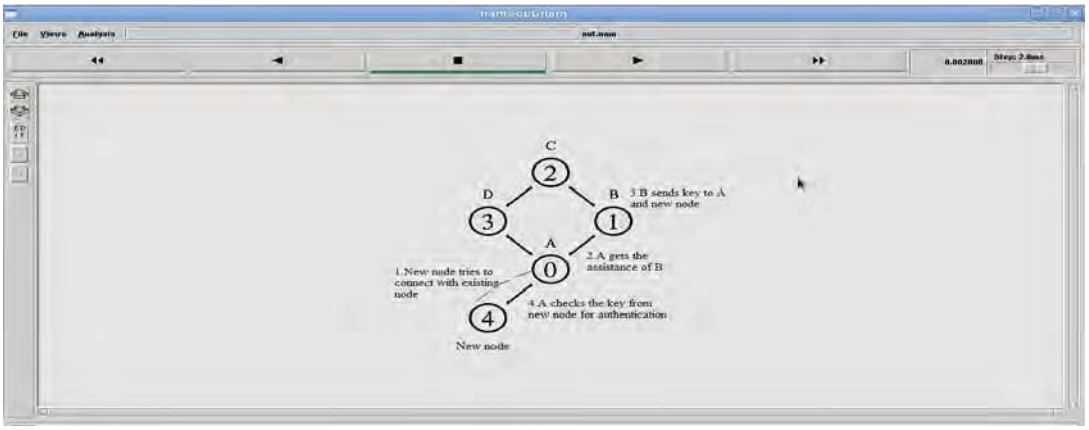


Figure 3: Neighbour Challenging.

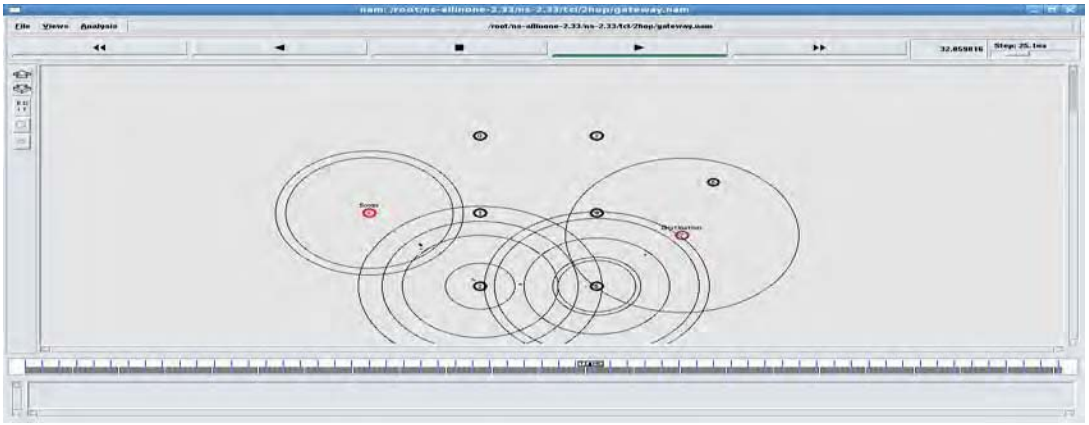

Figure 4: Routing through high rating nodes.

Figure 5 shows the statistical analysis of five test cases. The total number of nodes in the test cases is 15,25,12,35 and 19. For this total number of nodes, corresponding number of active and inactive nodes are mentioned. The analysis shows how many nodes are re-authenticated and average number of path found for routing. The fig. 6 is about the overcoming of drawback in the existing work, as test 1 has numerous number of malicious nodes and a limited number of paths by using existing mechanism but no malicious nodes and more number of paths found by the use of proposed mechanism. It avoids congestion due to more number of paths found.

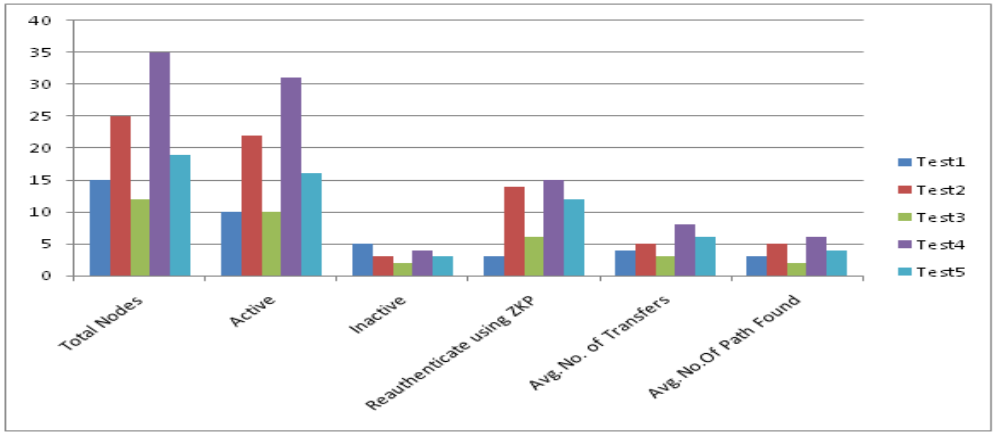


Figure5: Number of nodes re-authenticated and Number of paths found.

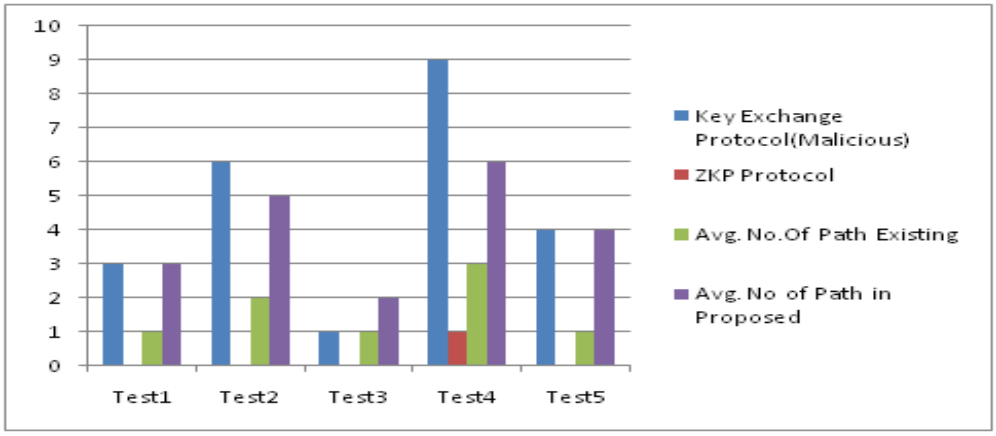


Figure 6: Increased number of paths reduces congestion.

In figure 7, existence of malicious nodes by using the previous work is shown. They are identified by the proposed work. The percentage of malicious nodes in existing work is calculated based on the presence of malicious nodes using key exchange mechanism and total number of nodes. A malicious node in proposed work is obtained from the presence of malicious nodes using ZKP and total number of nodes. The proposed system works well against malicious nodes.

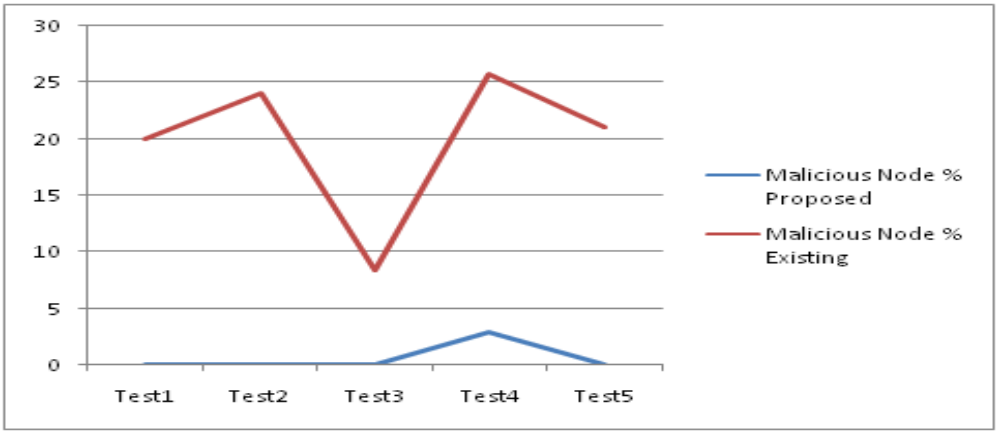


Figure 7: Performance analysis of existing with proposed system.

## V. CONCLUSION

The existing methodology does not address the re-authentication mechanism and also routing based on data rating only. The proposed methodology addresses these drawbacks. If one node is relieved from the authenticated ad-hoc network, it needs to be rejoining after some time. In order to rejoin, it has to be re-authenticated so as to verify it as trusted party. The routing mechanism is not only based on the transformation

of data quantities but also on RTT and RSS values. It is more dynamic, less overhead and vigor mechanism. As this way, the proposed methodology effectively overcomes the obstacles.

## REFERENCES


[1] Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow, IEEE, Karan Verma, Pushkar Gupta, and Pravina Dhurander, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE Systems Journal, Vol. 5, No. 2, June 2011.

[2] Natarajan Meghanathan, "A location prediction based routing protocol and its extensions for multicast and routing in mobile ad hoc networks", Ad Hoc Networks, Volume 9, Issue 7, September 2011, Pages 1104-1126.

[3] M. Tamer Refaei, Vivek Srivastava, Luiz DaSilva, Mohamed Eltoweissy, "A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks" The second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services(MobiQuitous'05), Page(s) 3-11, 2005.

[4] Kimaya Sanzgiri, Bridget Dahill, Brain Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", 10th IEEE International Conference on Network Protocols(ICNP'02), Page(s): 78-87, 2002.

[5] Wu, Xi; Liu, Si; Zhu, Huibiao; Zhao, yongxin; Chen, Lei;, "Modeling and Verifying the Ariadne Protocol Using CSP", Engineering of Computer Based Systems (ECBS), 2012 IEEE 19th International Conference and Workshops on 11-13 April 2012, Page(s): 24-32.

[6] Rajashekhar C. Biradar, Sunilkumar S. Manvi, "Neighbor supported reliable multipath multicast routing in MANETs", Journal of Network and Computer Applications, Volume 35, Issue 3, Pages 1074-1085, May 2012.

[7] Themistoklis Haniotakis, Spyros Tragoudas, Constantinos Kalapodas, "Security enhancement through multiple path transmission in ad hoc networks", Communications, 2004 IEEE International Conference, Vol. 7, Page(s): 4187-4191, 2004.

[8] Zouridaki C, Mark BL, Hejmo M, Thomas RK, "Robust cooperative trust establishment for MANETs", Proceedings of the fourth ACM workshop on security of ad hoc and sensor networks, Page 23-34, 2006.

[9] Lee SJ, Su W, Gerla M, "On-demand multicast routing protocol in multihop wireless mobile networks", Mobile Networks and Applications 2002; 7:441-53.

[10] George C. Hadjichristofi, Luiz A. DaSilva, Scott F. Midkiff, Unghee Lee, Waltemar De Sousa, "Routing, security, resource management, and monitoring in ad hoc networks: Implementation and integration", Computer Networks, Volume 55, Issue 1, Pages 282-299, 7 January 2011.