Research Journal of **Information Technology**

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 402-410, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.402.410

NIZKP to Achieve Authentication in *Ad-hoc* Networks

S. Samundeeswari and V.S. Shankar Sriram
School of Computing, SASTRA University, India

Corresponding Author: S. Samundeeswari, School of Computing, SASTRA University, India

ABSTRACT

Authentication in Mobile *ad-hoc* Networks (MANETs) is difficult and challenging because of its frequent topology changes. Central authority based authentication schemes have been proposed and with every movement of a node outside the network demands re-authentication of the nodes by the central authority before the node rejoins the network. This research contribution intends to propose a novel Non-Interactive Zero Knowledge Protocol (NIZKP) to address this problem of re-authentication. The proposed NIZKP achieves re-authentication by neighborhood authentication of the node that wants to rejoin the network. This reduces the dependences on the central authority for re-authentication thereby avoiding the attacks that are possible during re-authentication.

Key words: Authentication, zero knowledge proof, neighborhood verification, *ad-hoc* networks

INTRODUCTION

Security features like confidentiality, integrity and authentication plays a vital role in any form of communication be it wired or wireless. Authentication becomes difficult in a wireless network that doesn't have a fixed infrastructure and where the nodes of the network are mobile. Such types of wireless networks, where there is a lack of infrastructure and the mobility of nodes are frequent are termed as Mobile *ad-hoc* Networks (MANETs). In a MANET the nodes exhibit dynamic feature in terms of location (mobility) through which the nodes produce continuous nodes insertions and deletions (Kumar *et al*., 2011). So only the credential nodes can carry out the required tasks in a self-organized manner (Maity and Hansdah, 2012). This makes authentication a great challenge as it is not supported by any fixed infrastructure. The major problem in ensuring security service in an MANET lies on managing the keys and providing privacy for data communication. One cannot ensure security services in a MANET without the basic knowledge of solid key management. In this research contribution an attempt has been made to achieve re-authentication of nodes in MANET using a NIZKP (Non Interactive Zero Knowledge Protocol). Re-authentication happens when an authenticated node wants to rejoin the network after it has lost its connectivity due to mobility.

Now-a-days people are very much inclined towards the term "wireless" which enables the users to connect to his network regardless of the time and place. In order to achieve this, the researchers (Sengan and Pandian, 2012) turned their concentration over IP network configuration integrated with IP based network core and a set of networks that access it, which paved the way for the 4th generation communications with number of heterogeneous wireless access networks to come into play (Salmanian *et al*., 2010). Here the authentication plays a vital role to allow only the legitimate users to access the resources.

A MANET is a set of mobile computing nodes which communicate within themselves without the support of fixed infrastructure or a centralized administration (Stieghtz and Fuch, 2011). These nodes can meet anywhere, form a network and have a direct communication between each other by using radio technologies such as Bluetooth, IEEE 802.11 or HIPERLAN. Every node in the MANET behaves like a router as well as a host (Al-Bahadili *et al.*, 2011). The security challenges in MANET arise due to its dynamic nature, vulnerable links and *ad-hoc* environment. MANET has been used in sensitive applications such as search and rescue mission in military, sensor networks, etc. The major security issues to be focused in MANET are authentication, integrity and confidentiality (Martinez *et al.*, 2010).

In MANET, due to its mobility a node can join or leave the network in a dynamic fashion. So it becomes very difficult to control the user access as well as hard to define encryption technology. The nodes in this type of network can be attacked easily by inactive eavesdropping or active intervention (Chowdhury and Neogy, 2011). So each node should be able to confront the attacker in any form. There are various methods in research for secure authentication and cipher key management to overcome this vulnerability. The ID based technology provides authentication without prior information or any public key means that, it provides authentication without shared information. It avoids third party to pretend like the authorized user or re-using the authentication ID. The following authentications are needed for *ad-hoc* network:

- **Node authentication:** The insertion and deletion of node in MANET is frequent, so the third party camouflage is prevented by this node authentication
- **Confidentiality and integrity:** The data encryption is handled by establishing session keys

The intended readers may read Nikos Komninos *et al.* (2007) for more information on MANETs.

Most of the popular authentication protocols in MANET are based on one of the following. Mechanisms based on Authentication management architecture developed on RSA signature (Murugan and Shanmugam, 2011), Using Trusted Third Party (TTP) based authentication, identification schemes based on chain of trust (Irshad *et al.*, 2010). Location-limited authentication used when the area is small and physical authentication is needed between the closer nodes are the current authentication schemes.

One of most important characteristics of the *ad-hoc* network is group based applications, for these applications the traditional identification techniques discussed above may not be appropriate always. Fulfilling these requirements, leads to the development of the latest technique based on Non Interactive Zero Knowledge Proofs (NIZKPs) and solves the problem of authentication and self-organization for MANET nodes. The problem of re-authentication when a node moves out of a network and wants to rejoin the same network is not addressed by these existing mechanisms.

MATERIALS AND METHODS

Zero knowledge proof (ZKP): Zero knowledge proofs are cryptographic protocols which do not reveal the secret information during the execution of the protocol, the two parties sender and verifier communicate with each other interactively by many transactions, at the end of the execution of the protocol the verifier will be convinced by the prover that the prover knows the secret without revealing the secret itself to the verifier. The major categories of ZKPs are Zero Knowledge Interactive Proof (ZKIP) and Non Interactive Zero Knowledge Proof (NIZKP). A NIZK proves the knowledge of the secret without interaction by polynomially bounded verifier who reads the proof without revealing any information about the secret (Lapidot and Shamir, 1990). Here, a public communication-application (random string) is shared between the prover and the verifier. In order to protect from Denial of Service (DOS) attacks, although the communication-Application is publicly readable, may be sent only by the legitimate on-line members of the network and it is necessarily synchronized by the on-line nodes.

In the proposed scheme an on-line communication-application, provides us the status information of the node, through which all the legitimate nodes will send messages to the other live nodes in the network for publishing the information about the changes in the network. Secrecy will not be needed for this communication-application because it is meaningless for illegitimate nodes. This information is only needed for updating authentication information. This global information is updated periodically and stored by each live node in the form of a queue, which also allows the authentication of non live legitimate nodes whose access is authorized by the live node. The duration limit for an off-line node is decided by all the legitimate nodes of the network.

At the initial stage each member joins the network using a secret piece of information. These legitimate nodes have to prove their identity through the knowledge of the secret, without revealing any of the related information during the execution of the protocol by challenge and response. Here it becomes impossible for any adversary to steal the meaningful information, transmitted between the participating nodes, even if he gets the information from the communication-application.

When a node wants to rejoin an existing *ad-hoc* network it should prove its identity to its neighbor nodes to access the applications and to utilize the resources. Figure 1 depicts the same. This can be achieved by our Non Interactive Zero Knowledge Protocol (NIZKP) authentication procedure. If this had not been the case, every time a node that wants to rejoin has to prove its identity to the Central Authority (CA). This requires additional network bandwidth in terms of messages communicated between the node and the CA resulting in overhead. The key advantage in NIZKP is that any valuable information will never be revealed during the communication and also reduction in the computational power by reducing the several rounds of interaction between the nodes since it is non interactive nature.

Proposed NIZKP protocol: The incoming node X who wants to rejoin the *ad-hoc* network should prove its identity to the neighbor nodes B and c in the following way:

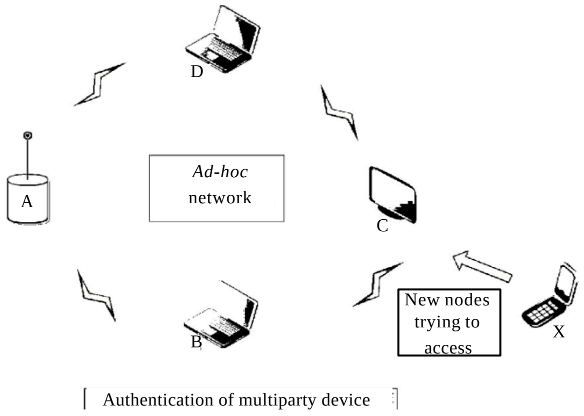
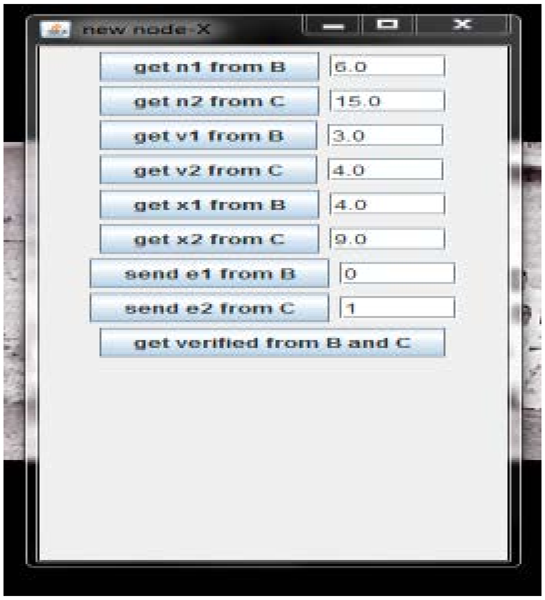

D
A
Ad-hoc network
C
New nodes trying to access
X
B
Authentication of multiparty device

Fig. 1: Re-authentication in MANET



get n1 from B 6.0
get n2 from C 15.0
get v1 from B 3.0
get v2 from C 4.0
get x1 from B 4.0
get x2 from C 9.0
send e1 from B 0
send e2 from C 1

Fig. 2: X gets challenge values from B and C

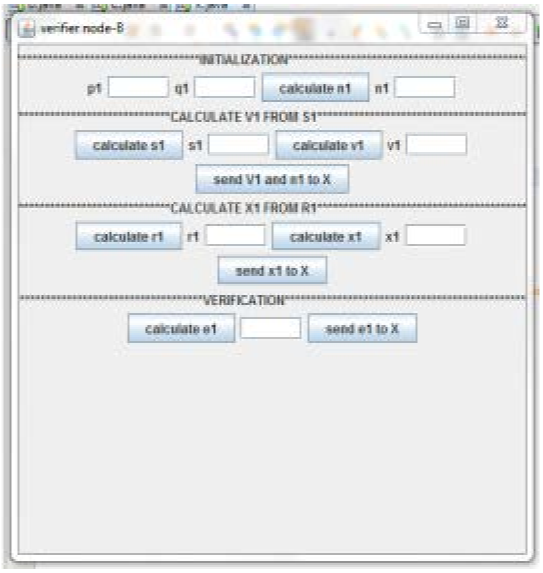
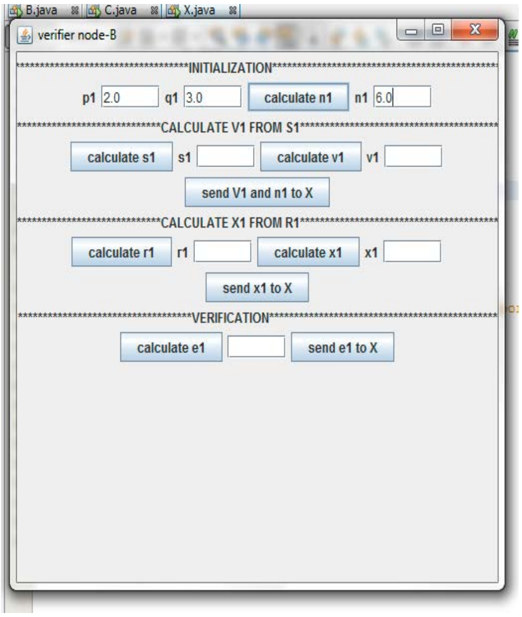


Fig. 3: X gets n1 and n2 values from B and C

Step 1: The new node x's secret keys are s_1 and s_1 and X will choose two random numbers m1 and m2 such that m1>s1 and m2>s2. Now x sends m1 to B and m2 to C. This forms the basis of the challenge process which is shown in Fig. 2

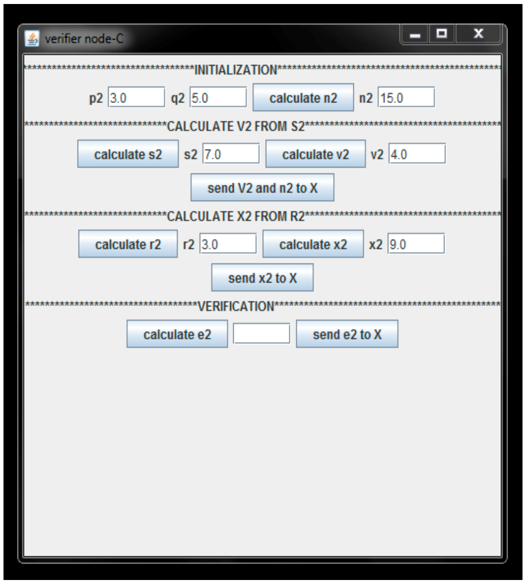
Step 2: Node B and C will choose prime numbers p_1, q_1 and p_2, q_2 such that their multiplications n_1, n_2 are greater than m1 and m2 and sends the values of n1 and n2 to node X. This is shown in Fig. 3

Step 3: The new node X computes v1 and v2 such that:



p1 2.0 q1 3.0 n1 6.0

Fig. 4: X computes v1 and v2 values



p2 3.0 q2 5.0 n2 15.0

s2 7.0 v2 4.0

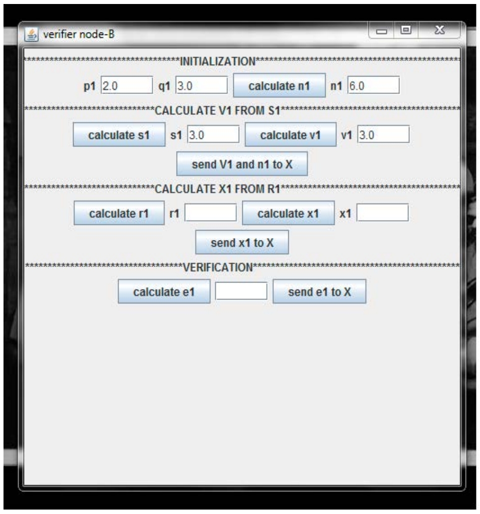
r2 3.0 x2 9.0

Fig. 5: X sends x1 and x2 values to B and C

$$v_1, = s^2{}_1 \text{ mod } n_1, \; v_2 = s^2{}_2 \text{ mod } n_2$$

To prove its identity to B and C, The public keys are (v1, n1) and (v2, n2). This is shown in Fig. 4

Step 4: The node X chooses two random numbers r1 from {1, 2, ..., n1-1} and r2 from {1, 2, ..., n2-1} with uniform distribution and computes $x_1 = r_1^2$ mod n_1 and $x_2 = r_2^2$ mod n_2. Now X sends x1 to B and x2 to C. This is shown in Fig. 5



verifier node-B

INITIALIZATION

p1 2.0 q1 3.0 n1 6.0

CALCULATE V1 FROM S1

s1 3.0 v1 3.0

CALCULATE X1 FROM R1

r1 x1

VERIFICATION

Fig. 6: B sends V1 and n1 to node X

Step 5: The nodes B and C chooses their challenge values e1, e2 from {0, 1}, respectively with the uniform distribution and node B sends e1 to X and node C sends e2 to x

Step 6 (for node 'B'): If node B sends e1 value as 0, then the new node X sends the response, the random number r1, to B. Node B verifies $r_1^2 = x_1 \bmod n_1$. This is shown in Fig. 6

Else if the node B sends e1 value as 1, then the new node sends the response as $y_1 = r_1 s_1 \bmod n_1$, to node B. Now, node B verifies $y_1^2 = x_1 v_1 \bmod n_1$.

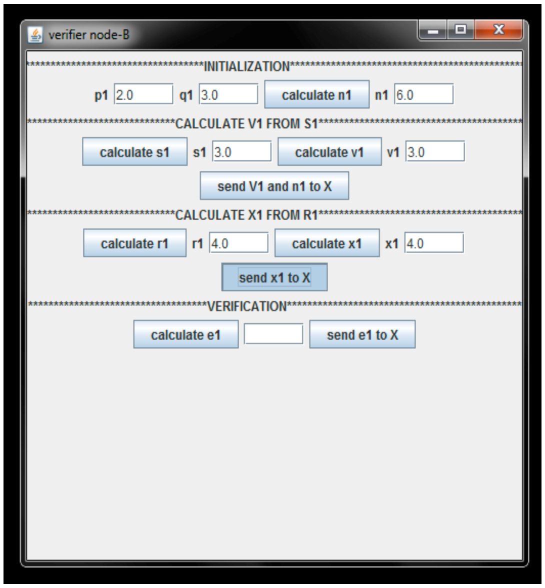
Step 7 (for node 'C'): If the node C send e2 value as 0, then the node X sends the response as $y_2 = r_2 s_2 \bmod n_2$, to node C. Then node C verifies $y_2^2 = x_2 v_2 \bmod n_2$

Else the node C send e2 value as 1 from node C then the node X sends the response, random number r2 to node C. Node C verifies $r^2_2 = x_2 \bmod n_2$. This is shown in Fig. 7.

Step 8: If both the nodes B and C are satisfied with the incoming node's (X) identity, then X is allowed to communicate. Ib and Ic = Ix, where 'and' denotes "Logical AND operation". Once the authentication of s1 and s2 has been successfully carried out the node x will communicate with the network and access the resources as represented in Fig. 8 and 9

Illustration: Let us consider an *ad-hoc* network with n number of nodes, if a new node X wants to rejoin the network, it gets authenticated by the closest/neighbor nodes B and C, making node X is a valid node. Once node X has been authenticated, it starts its communication among the nodes in the *ad-hoc* network.

Step 1: New node X private keys are s1 = 3 and s2 =7. It chooses 2 random numbers m1 and m2, such that m1 = 5>s1 and m2 = 9>s2. Then node X sends m1 to node B and m2 to node C, respectively

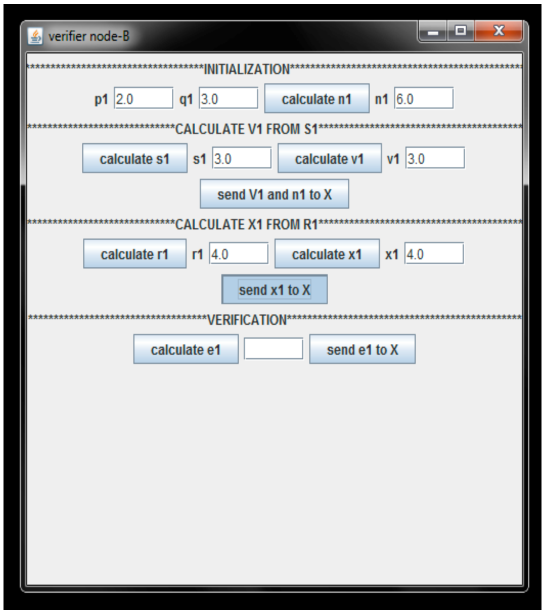


p1 2.0 q1 3.0 n1 6.0

s1 3.0 v1 3.0

r1 4.0 x1 4.0

Fig. 7: C calculates x2 and r2



p1 2.0 q1 3.0 n1 6.0

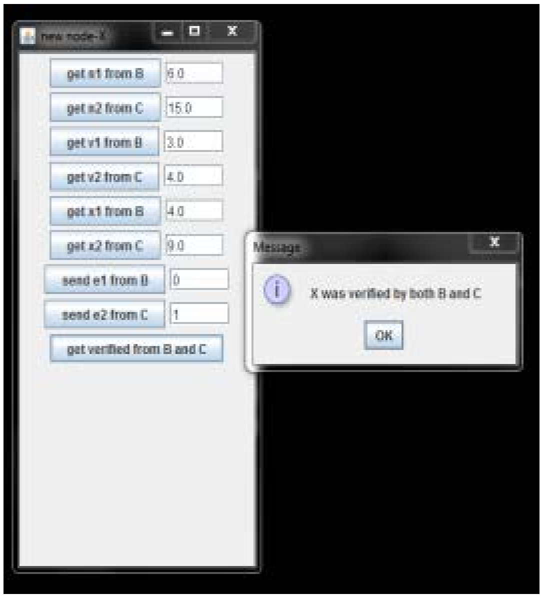
s1 3.0 v1 3.0

r1 4.0 x1 4.0

Fig. 8: C calculates p2, q2 and n2 values

Step 2: The nodes B and C chooses 2 large prime numbers p1 = 2, q1= 3 and p2 = 3, q2 = 5, then calculates n1 = p1* q1 = 6 and n2 = p2* q2 = 15. Node B sends n1 to X and node C sends n2 to X

Step 3: The new node X computes v1 and v2 such that, $v_1 = s_1^2 \bmod n_1 v_2 = s_2\,^2\bmod n_2 = 15$, respectively, Now the 2 public keys of the node x are (v1, n1) = (3, 6) and (v2, n2) = (4, 15)



get n1 from B 6.0
get n2 from C 15.0
get v1 from B 3.0
get v2 from C 4.0
get x1 from B 4.0
get x2 from C 9.0
send e1 from B 0
send e2 from C 1

X was verified by both B and C

Fig. 9: B and C verified the node X

Step 4: The node X chooses two random numbers r1 = 4 and r2 = 3 and computes $x_1 = r^2_1$ mod $n_1 = 4$ and $x_2 = r^2_2$ mod n = 9. Now X sends x1 to B and x2 to C

Step 5: The nodes B and C chooses the challenge values e1 = 0, e2 = 1, then node B sends e1 to X and node C sends e2 to X

Step 6: The new node x sends the random number r1 = 4 to node B. Then node B verifies that $r^2_1 = x_1$ mod $n_1 = 4$. Likewise node X calculates $y_2 = r_2s_2$ mod $n_2 = 6$ and sends to the node C. Then node C verifies that $y^2_2 = x_2v_2$ mod $n_2 = 6$

Once the verification of the node x has been done by the nodes B and C node x allowed to communicate with the other nodes in the network.

Security analysis: The following are the facts of security analysis:

- In MANETs due to the of lack of centralized structure the Denial of Service (DOS) attacks are natural. In order to protect the nodes from the DOS attack it is better that the public communication-application is made available only to the legitimate nodes of the network
- The proposed system is resistant to identity theft as the node access is controlled by NIZKP. Here the man-in-the-middle attack is avoided as there is no way to gain any information during the transaction
- The most dangerous attack in the MANET is sibling attack which occurs when a node uses multiple identities and even it leads to false centralized authority, this major problem is avoided in NIZKP because of its distributed nature

SIMULATION AND DISCUSSION

The proposed protocol was simulated using Java Sockets. The node-X is the one who wants to rejoin the network, hence is the prover. Nodes B and C are the ones who authenticate the node-X, hence are the verifiers.

CONCLUSION

This contribution proposed a new re-authentication scheme for MANETs using knowledge based member authentication without the necessity of CA using NIZKP which do not reveal any useful information during the protocol execution. The simulations results for the proposed protocol make it evident that the protocol is foolproof.

REFERENCES

Al-Bahadili, H.A., S.M.B. Hussain, G.B. Issa and K.C. El-Zayyat, 2011. Performance evaluation of the TSS node authentication scheme in noisy MANETs. Int. J. Network Secur., 12: 121-129.

Chowdhury, C. and S. Neogy, 2011. Mobile agent security in MANET using reputation. Proceedings of the 1st International Conference on Parallel, Distributed Computing Technologies and Applications, September 23-25, 2011, Tirunelveli, India, pp: 158-168.

Irshad, A., W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad and M. Usman, 2010. Security enhancement for authentication of nodes in MANET by checking the CRL status of servers. Proceedings of the 1st International Conference on Security-Enriched Urban Computing and Smart Grid, September 15-17, 2010, Daejeon, Korea, pp: 86-95.

Komninos, N., D. Vergados and C. Douligeris, 2007. Detecting unauthorized and compromised nodes in mobile *ad-hoc* networks. *ad-hoc* Networks, 5: 289-298.

Kumar, V.A., R.B. Sharma and A.C. Kush, 2011. Key authentication for MANET security. Proceedings of the International Conference on High Performance Architecture and Grid Computing, July 19-20, 2011, Chandigarh, India, pp: 497-504.

Lapidot, D. and A. Shamir, 1990. Publicly verifiable non-interactive zero-knowledge Proofs. Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, August 11-15, 1990, Santa Barbara, California, USA., pp: 353-365.

Maity, S. and R.C. Hansdah, 2012. Membership models and the design of authentication protocols for MANETs. Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops, March 26-29, 2012, Fukuoka, Japan, pp: 544-551.

Martinez, P.M.R., R.M. Lopez, F.J. Ros and J.A. Martinez, 2010. Enhanced access control in hybrid MANETs through utility-based pre-authentication control. Wireless Commun. Mobile Comput., 10: 688-703.

Murugan, R.A. and A.B. Shanmugam, 2011. A cluster based authentication technique for mitigation of internal attacks in MANET. Eur. J. Sci. Res., 51: 433-441.

Salmanian, M.A., J.B. Hu, L.B. Pan , P.C.A. Mason and M.A. Li, 2010. Supporting periodic, strong re-authentication in MANET scenarios. Proceedings of the Military Communications Conference, October 31-November 3, 2010, San Jose, CA., USA., pp: 19-25.

Sengan, S.A. and S.B.C. Pandian, 2012. Authorized node detection and accuracy in position-based information for MANET. Eur. J. Sci. Res., 70: 253-265.

Stieglitz , S. and C. Fuch, 2011. Challenges of MANET for Mobile Social Networks. Procedia Comput. Sci., 5: 820-825.